GDPR STATEMENT

July 2023

TMF Group takes privacy of its (prospective) business relations, its (candidate) employees and other staff very seriously. We take meticulous care in protecting the personal data entrusted to us. To this effect we have enhanced and introduced new technical and organisational measures in order to comply with the data protection laws (General Data Protection Regulation (EU) 2016/679 ("GDPR") (EU) 2016/679 ("**GDPR**") together with all implementing laws and any other applicable data protection laws, privacy laws or privacy regulations).

Efforts TMF Group is undertaking to ensure enduring data protection laws compliance.

In order to ensure fair and transparent processing of personal data, taking into account the specific circumstances and context in which the personal data are processed, we have enhanced already available, and introduced new technical and organisational measures to prevent the misuse, unauthorised access to, modification, disclosure and destruction of personal data in order to ensure that factors which result in potential risks for personal data are minimized to the furthest extent.

To ensure compliance with data protection laws we have drafted new and updated existing internal policies and manuals, and implemented measures which meet in particular the principles of privacy by design and privacy by default. Such measures amongst other effect in: (i) minimised processing of personal data, (ii) increased security of processing, (iii) transparency with regard to the processed data, (iv) accommodating adequate and timely responses to data subject requests, (v) support for timely incident response procedures, and (vi) supervision of compliant personal data processing activities to ensure legitimate and adequate processing.

When developing, designing, selecting and using business applications, or rendering services and delivering products to our clients which include processing of personal data, we ensure to fulfil our legal obligations with respect to data protection laws. The principles of privacy by design and privacy by default are respected throughout the process, and organisational and technical measures principally undertaken by TMF Group -as listed below- are also continuously being evaluated and improved.

Data protection laws related organisational measures

- Privacy governance framework has been set-up, introducing the role of the Global Privacy Team, who are ensuring data protection laws compliance and compliance with local privacy laws throughout the jurisdictions we operate in.

- Global Privacy Team consisting of the Group Privacy Office, the Head of Risk and Compliance, the Group Directors Legal, Market Heads of Legal and Market Head of Risk and Compliance, Country Privacy Leads and the Data Protection Officers, where appointed, was established to enhance the data protection laws compliance throughout the jurisdictions we operate in.
- External and internal privacy policies and statements reflect the data protection laws' requirements.
- We have implemented processes, procedures and guidelines to support our clients, prospects, candidate employee' and employee' requests with their data subject rights under Chapter III GDPR and applicable data protection laws such as right to data portability, right to erasure ('right to be forgotten'), right to information and transparency, the right of access and rectification, the right to restrict processing and the right to object to (automated) personal data processing.
- Data inventory (records of processing activities, "**RoPA**") has been set-up by reputable and industry-leading experts in accordance with the financial industry best practices. It is being maintained in compliance with data protection laws and provides a view on the data flows throughout the organisation. The required updates of RoPA are rooted in the organisational processes.
- Data Protection Impact Assessments ("**DPIA**") is carried out as required and upon request - to support clients' compliance. For internal processes DPIA quick scans and DPIA's are carried out before starting any high risks processing activities.
- Guidelines, procedures and processes are in place to handle security incidents involving or affecting personal data. These procedures and resolution of incidents are supervised by the Group Privacy Office and Security Officers.
- Service agreements and respective data processing agreements with our clients and suppliers (subprocessors) reflect the data protection laws requirements. We seek to only engage subprocessors which provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, and require from them to implement technical and organisational measures which meet the requirements of data protection laws and our clients, including for the security of processing. Our agreements with these service providers do not permit use of your personal data for their own (marketing) purposes. Consistent with applicable legal requirements, we take commercially reasonable steps to require third parties to adequately safeguard your personal data and only process it in accordance with our instructions.
- The lead data protection supervisory authority of TMF Group located in the Netherlands ("De Autoriteit Persoonsgegevens") has approved TMF Group Binding Corporate Rules for international data transfers, both controller and processor version. The fact of approval is published on the website of the European Commission.
- Data protection laws compliance of each TMF Group affiliate is subject to regular internal audits under supervision of Group Privacy Office.
- Trainings and awareness campaigns directed to all Employees are being carried out on regular basis, and all Employees are required to complete the mandatory GDPR trainings which are updated on an annual basis.

- TMF Group direct marketing campaigns are data protection laws ready, meaning that they are carried out with prior privacy-oriented assessment and under supervision of data privacy trained marketing professionals.

Data protection laws related technical and security measures

- All staff has signed confidentiality statements, and it is required to adhere to internal policies.
- Staff's activity on and access to IT systems and physical personal data storage facilities ("**Storage**") is secured, aligned with (multiple) authentication requirements and separable.
- A division of staff roles and responsibilities is implemented that reduces the possibility for a single individual to compromise a critical process.
- Every member of the staff is only performing authorized duties relevant to its respective jobs and positions.
- In the IT security and cybersecurity context proportional and appropriate measures of data at TMF Group are taken.
- Implemented cybersecurity measures are appropriate to the size and use of our network, as well as the organisation information system.
- Staff access rights to IT systems and Storage are in line with predefined and documented business needs, and the job requirements are attached to user identities.
- Staff account management is restricted to authorized personnel and reviewed on a periodic basis.

We encourage clients, suppliers and partners to review our data protection laws compliant **Personal Data Protection Policy** and supporting **Statement of Continuity** containing description of TMF Group technical and security measures in place along with **Binding Corporate Rules** which enable us to transfer the personal data intra-group without any further legal or technical restrictions.

For all other contracting enquiries please don't hesitate to contact your local office or our dedicated team on dataprotection@tmf-group.com.

GDPR Statement – TMF Group | June 2018 | Version 1.0

GDPR Statement – TMF Group | July 2023 | Version 2.0