Privadium GDPR Statement

Privadium 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 organizational measures in order to comply with the General Data Protection Regulation (EU) 2016/679 ("GDPR").

Efforts Privadium is undertaking to ensure enduring GDPR 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 organizational measures to ensure that factors which result in potential risks for personal data are minimized to the furthest extent.

To ensure compliance with GDPR, 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) minimized 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 GDPR. The principles of privacy by design and privacy by default are respected throughout the process, and organizational and technical measures principally undertaken by Privadium -as listed below- are also continuously being evaluated and improved.

GDPR related organizational measures
Privacy governance framework has been setup, introducing the role of the Chief Privacy Officer and the Global Privacy Team, who are ensuring GDPR compliance and compliance with local privacy laws throughout the jurisdictions we operate in.
External and internal privacy policies and statements have been updated to reflect the GDPR requirements.
We have implemented processes, procedures and guidelines to support our clients, prospects and employee' requests with their so-called Chapter III GDPR rights: 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 GDPR and provides a view on the data flows throughout the organization. The required updates of RoPA are rooted in the organizational processes;
Data Protection Impact Assessments ("DPIA") can be 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 incidents involving personal data. These procedures and resolution of incidents are supervised by our Privacy and Security Officers.

Service agreements with our clients and suppliers (sub-processors) reflect the GDPR requirements. We seek to only engage sub-processors which provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, and require from them to implement technical and organizational measures which meet the requirements of GDPR and our clients, including for the security of processing.

Dutch (Privadium leading) supervisory authority approved Privadium Binding Corporate Rules (BCRs) for controller and processor intra-group transfers of personal data to and from countries which offer inadequate level of protection compared to the one applicable in the European Union.

GDPR compliance of each local office is subject to regular internal audits under supervision of Chief Privacy Officer.

Trainings and awareness campaigns directed to all employees have been carried out, and all employees are required to complete the mandatory GDPR training. The trainings are being updated on an annual basis.
Privadium direct marketing campaigns are GDPR ready, meaning that they are carried out with prior privacy-oriented assessment and under supervision of GDPR trained marketing professionals.

GDPR 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.

- 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 GDPR compliant Personal Data Protection Policy and supporting Statement of Continuity containing description of Privadium 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@privadium.com.