

# GDPR COMPLIANCE STATEMENT

## 1. INTRODUCTION

The **EU General Data Protection Regulation ("GDPR")** comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardize data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

## 2. OUR COMMITMENT

**Trustifi** ('we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognize our obligations in updating and expanding this program to meet the demands of the GDPR.

**Trustifi** is dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarized in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

## 3. HOW WE ARE PREPARING THE GDPR

**Trustifi** already has a consistent level of data protection and security across our organization, however, it is our aim to be fully compliant with the GDPR by June 30, 2019. Our preparation includes:

- **Information Audit** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- **Policies & Procedures** - revising and implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
  - **Data Protection** – our main policy and procedure document for data protection have been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
  - **Data Retention & Erasure** – we have updated our retention policy and schedule to ensure that we meet the 'data minimization' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
  - **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our

procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

- **International Data Transfers & Third-Party Disclosures** – In certain circumstances, we will transfer personal data information outside of the European Economic Area, including to the United States of America. Where we do so, we will ensure appropriate safeguards are in place, including, for example, that the third parties we use who transfer your information outside the European Economic Area have self-certified themselves as compliant with the EU-U.S. Privacy Shield. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- **Subject Access Request (SAR)** – we have written our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- **Legal Basis for Processing** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR. Our Legal Basis for Processing is contracts and consent.
- **Privacy Notice/Policy** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining Consent** - we are revising our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- **Direct Marketing** - we are revising the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- **Data Protection Impact Assessments (DPIA)** – where we process personal information that is considered high risk, involves large-scale processing or includes a special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- **Processor Agreements** – where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, hosting etc.), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organizational measures in place and compliance with the GDPR.
- **Special Categories Data** - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition.

## 4. DATA SUBJECT RIGHTS

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website – <https://trustifi.com> of an individual's right to access any personal information that **Trustifi** processes about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

## 6. INFORMATION SECURITY & TECHNICAL AND ORGANISATIONAL MEASURES

**Trustifi** takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction and have several layers of security measures, including:

- All **Trustifi** network traffic, whether it contains PHI or not, is encrypted using industry-standard transport encryption (TLS). Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS 1.1 and TLS 1.2 protocols ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). SSLv2, SSLv3, and TLS 1.0 are no longer considered secure protocols and thus are not used or supported by **Trustifi**.
- **Trustifi** have implemented technology and security policies and other measures to protect the personal data to her customers from unauthorized access, improper use, alteration, unlawful or accidental destruction, and accidental loss. **Trustifi** also requires all her employees and others who have access to or are associated with the processing of your data respect your confidentiality.

## 7. GDPR ROLES AND EMPLOYEES

**Trustifi** have designated **Mark Liapustin as Data Protection Officer (DPO)** to develop and implement **Trustifi** roadmap for complying with the new data protection Regulation. The DPO is responsible for promoting awareness of the GDPR across the organization, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures, and measures.

**Trustifi** understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to GDPR and Information Security Awareness.

If you have any questions about our preparation for the GDPR, please contact the **Data Protection Officer (DPO)** – **Mark Liapustin** at [mliapustin@trustificorp.com](mailto:mliapustin@trustificorp.com)