GDPR Compliance Statement

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 new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

Universal Smart Cards is committed to ensu ring 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 recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Laws.

Universal Smart Cards 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 summarised 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.

How Universal Smart Cards has prepared for the GDPR

Universal Smart Cards already has a consistent level of data protection and security across our organisation, however it has been our aim to be fully compliant with the GDPR by 25th May 2018 or as soon as practibly possible thereafter. ***Our preparation included: -***

- ***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 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 has 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 minimisation'* 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*** – Universal Smart Cards manufactures and handles anonymous cards (ie "unpersonalised") smart cards, as well as printing and encoding names, job titles and other personal data ("personalised"). We have a policy to process personlaised cards in the UK where at all possible. Where **Universal Smart Cards might** store or transfer personal information outside the EU, we will conduct a case by case risk assessment to ensure that we will have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our assessment will include a review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without.
- ***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 and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we are revising our Privacy Notice 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.
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf, 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 organisational measures in place and compliance with the GDPR.
- ***Terms and Conditions of Sale*** – we have updated our Terms to reflect the new environment under GDPR
- ***Registration with ICO –*** We have registered with the ICO. Our Certificate of Registration is available on request.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we will provide easy to access information for instance via email requests, speaking to relevant individuals and during induction of an individual's right to access any personal information that Universal Smart Cards 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

Information Security & Technical and Organisational Measures

Universal Smart Cards takes the privacy and security of individuals and their personal information very seriously and take 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 unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:-

- **SSL**
- **SFTP**
- **Access controls**
- **Password policy,**
- **Encryption**
- **Practices,**
- **Restriction**
- **IT**
- **Authentication**

GDPR Roles and Employees

Universal Smart Cards has designated **Kevin Loveman** and **Paul May** as our **Appointed Persons** to develop and implement our roadmap for complying with the new data protection Regulation. They have been responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Universal Smart Cards 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 the which will be provided to all employees prior to May 25th, 2018, and it now forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact our Appointed Persons.