Prepaid Financial Services Ltd 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. Founded on the fundamentals of privacy by design and a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st century brings with it, the broad use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. 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

Prepaid Financial Services Ltd (PFS) *('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 framework in place which complies with existing law and abides by the data protection principles. However, we recognise the requirement and importance of updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

PFS is dedicated to safeguarding the personal information under our responsibility and to developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation plans for the GDPR have been summarised in this statement and includes the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum compliance at all times.

How We are Preparing for the GDPR

PFS already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by **25th May 2018**.
Our preparation includes: -

- *Information Review* - carrying out a company-wide information review to identify and assess what personal information we hold, where it comes from, how and why it is processed, and if disclosed, 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 is being 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 focus on the rights of individuals.
    - *Data Retention & Erasure* – we are updating 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 will 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 to this, like ensuring we comply with anti-money laundering

obligations to retain data relating to financial transactions for 5 years, 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 opportunity. Our procedures are robust and will be distributed to all employees, who are aware of the reporting lines and steps to follow. We are updating current policies to comply with the requirement to report security breaches within 72 hours, to our supervisory authority, the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- *International Data Transfers & Third-Party Disclosures* – where PFS stores or transfers personal information outside the EU, we already have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. We will complete continual reviews of the countries with sufficient adequacy decisions, like the Privacy Shield in the US, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct. We carry out due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information.
- *Subject Access Request*– we are updating our Subject Access Request procedures to accommodate the revised 1-month 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 and what exemptions apply.

- *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 are also maintaining records of our processing activities, ensuring that our obligations under Article 30 of the GDPR (Records of processing activities) are met.
- *Privacy Notice*– 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 on the CCP for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways for data subjects to consent to us processing their information. Our Terms and Conditions currently address the consent to use personal data, but this is changing to ensure we comply with Article 7 of the GDPR (Conditions for consent). We are developing processes for recording consent, making sure that we can evidence an agreeing opt-in, and a way to withdraw consent at any time for marketing purposes only. Consent cannot be withdrawn for data relating to financial transactions once activity begins. A revised version of the Terms and Conditions will be available soon for distribution to your clients and for your website. If you use your own platform instead of our ACP/CCP then you will need to make arrangements to gather consent from data subjects before you collect their data. This consent needs to be recordable and auditable to comply with the requirements.
- *Obtaining Parental Consent* – the GDPR states that where the child is below the age of 16 years, such processing shall be lawful only if consent is given or authorised by the holder of parental responsibility over the child. The GDPR does allow that Member States may provide by law for a lower age for those purposes, provided that such lower age is not below 13 years. In the UK Data Protection Bill, the age parental consent is required will be set to under 13, which means any minor that is 13 or over will be permitted to provide consent themselves without parental consent. The laws in each jurisdiction will vary so you will be required to have measures in place to capture consent depending on the rules around consent transposed into the local law in your area.
- *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.
- *Data Protection Impact Assessments (DPIA)* – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed a procedure and assessment template for carrying out impact assessments that comply fully with Article 35 of the GDPR (Data Protection Impact Assessments).

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights. Our Private Notice will provide easy to access information of an individual's right to access any personal information that PFS 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 (*only where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us.
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

Information Security & Technical and Organisational Measures

PFS takes the privacy and security of individuals and their personal information very seriously and we take every reasonable measure and precaution to protect and secure the personal data that we process. We have dedicated information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and security measures, including: -

PCI DSS certification
Access Controls
Encryptions
Pseudonymisation with CHIDs

GDPR Roles and Employees

PFS will have a designated Data Protection Officer (DPO) and have appointed a GDPR Project team to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation and programmes, assessing our GDPR readiness, identifying any gap areas and drafting and implementing the new policies, procedures and measures.

We utilise a GDPR checklist designed to assess each business activity, function and process and to ensure that we have a company-wide approach to meeting the new standards and requirements.

PFS understands that continuous employee and client awareness and understanding is vital to the continued compliance of the GDPR.

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

Thanking you
The PFS GDPR Project Team