Briefing Note: Worldpay's General Approach to Privacy and EU GDPR Implementation

Data Protection

Version:	Final
Issued on:	30 September 2016
Author	Andreas Klug, Group Data Privacy Officer Legal, Corporate Services, Data Protection

Table of Contents

1 Purpose

The purpose of this briefing note is to provide some general thoughts and guidance about Worldpay's connected approach to data, privacy and the EU General Data Protection Regulation ("**GDPR**").

2 Key messages

- Like many of its customers, Worldpay is an increasingly data driven business.
- Worldpay therefore views data as a critical asset that requires protection, governance and strategic attention.
- GDPR compliance will be central to our approach as will be compliance with other data laws that may apply to our business.

3 GDPR Compliance Strategy

3.1 General approach

- The precise nature of the impact that the GDPR is likely to have on Worldpay is currently being assessed.
- Any impact will, to some degree, depend on the outcome of the UK's exit negotiations with the EU and the data protection regime that will emerge following Brexit.
- In any event, the GDPR essentially reinforces privacy principles which have been in place for decades, so it is not an entirely new framework.
- What has changed is that many businesses, even those which started life as brick and mortar operations, are continuously increasingly their digital footprint and are considerably more data driven.
- This has led to a paradigm shift in the relevance of data to both our and our customer's businesses.
- The GDPR's aim is to update already existing frameworks such as the EU Data Protection Directive in order to reflect this new reality.
- Worldpay has already embedded the key principles mandated by the EU Data Protection Directive and other laws and regulations into its processes and operations.
- We are therefore confident that we already comply or are close to complying with many GDPR requirements.
- We are also in the process of undertaking a gap analysis to identify areas where additional work will be required to ensure compliance.

3.2 Key areas of focus

- Cyber security and data breach management:
    - Information security risk management framework - Worldpay is certified as compliant to ISO27001:2013;
    - Annual risk assessments covering cyber threat and physical & geo-political threats;
    - A bi-annual Security Advisory Board, with participation by Executive Board members and independent industry advisors;
    - Annual regulatory security awareness training for all staff, with supplementary campaigns throughout the year;
    - Pre-employment screening for all new hires and promotions to senior positions;
    - Security Incident and Crisis Management processes with supporting senior management team;
    - Cryptographic hardware measures (HSMs) in order to encrypt data at rest;
    - Robust role-based access control and strong password policies;
    - Two factor authentication for remote access with encrypted connectivity;
    - Network segmentation (towers and tiers), each protected by firewalls;
    - Dedicated management (IT admin) networks with two factor authentication and encrypted connections;
    - Centralised log collation and monitoring;
    - Advanced persistent threat protection;
    - Intrusion detection systems;
    - Anti-malware systems;
    - Data leakage protection;
    - Proxies for inbound and outbound traffic;

- Industry leading Distributed Denial of Service protection;
- 24*7 security operations;
- Daily external and internal vulnerability scans;
- Automated code review scanning capabilities;
- Systems development lifecycle assurance processes;
- Asset disposal processes in line with NIST SP800-88;
- Robust change management processes covering infrastructure, application and environmental changes;
- Segregation of duties, for example between development and production support communities; and
- Data replication between data centres, with critical systems supporting an active-active configuration.

- Continue to build privacy requirements into our systems, processes, projects and products (privacy by design/by default, use of privacy enhancing technologies).
- Data mapping and documenting our data processing activities.
- Assess our legal and compliance frameworks for data transfers and ensure alignment with our data flows.
- Build data governance frameworks to ensure a high degree of data integrity and quality through data hygiene and continued automation of processes e.g. customer onboarding, customer self-service portals.
- Mitigate data risk by only collecting data that is needed (data minimisation).
- Ensure transparency and choice of data processing through privacy notices, consent collection and tracking mechanisms.
- Utilise tools to de-identify and anonymise data where appropriate to reduce data risk and mitigate GDPR requirements.
- Develop anonymization methodology and use benchmarking rules to reinforce and enhance data anonymization and enable data analytics and other data driven products.
- Reinforce, as necessary, our supplier risk management framework.
- Raise data IQ within the business through continued and structured employee engagement programme which includes, online training modules, face-to-face sessions and webinars.