Apex GDPR Whitepaper

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.

Apex believes the GDPR is a significant step forward in data privacy and supports the GDPR's emphasis on strong data privacy protections and security principles. Apex is committed to ensuring that it is GDPR compliant when the law becomes enforceable on 25th May 2018 and is dedicated to helping our customers become GDPR compliant.

Our Commitment

Apex is dedicated to safeguarding our customer's personal information entrusted to us, developing our data protection program to be effective and fit for purpose, and demonstrating 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 or updated data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We Are Preparing for the GDPR

Apex already has a consistent level of data protection and security across our organization, and it is our aim to be fully compliant with the GDPR by 25th May 2018. Our preparation includes:

- *Product Review* – Making behind the scene changes to ensure that the Trajectory platform and services are GDPR compliant and support GDPR rights: including implementing changes focused on access controls, account and record deletion, security, storage, and audits. Apex is also internally working with our engineering, product, and security teams to ensure that we are able to help our customers respond to any data subject requests that they may receive and proactively ensure GDPR compliance for every new product or enhancement.

- *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. We have a dedicated focus on privacy by design, data privacy principles and data subject rights.

    - *Data Retention & Erasure* – We are updating 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 are developing erasure procedures 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 in accordance with the GDPR. 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* – Where Apex stores or transfers personal information outside the EU, we have procedures and safeguarding measures in place to secure, encrypt and maintain the integrity and confidentiality of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; we have standard data protection clauses or approved codes of conduct for those countries without. 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 revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our updated procedures detail how to verify the data subject, what steps to take for processing an access request, and what exemptions apply 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 and Schedule 1 of the Data Protection Bill are met.

- *Privacy Notice* – We are revising 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.

- *Data Protection Impact Assessments (DPIA)* – Where we process personal information that is considered high risk, involves large scale processing or includes special category data, we have developed 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, we are enforcing Data Protection 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.

Apex Employees' GDPR Roles

Apex has identified the key stakeholders within the organization to develop and implement our roadmap for complying with the new data protection regulation. The team 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.

Apex understands that continuous employee awareness and understanding is vital to the continued compliance with the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to GDPR which will be provided to all employees prior to 25th May 2018, and forms part of our annual training program.

Customer Responsibilities

Compliance is a shared responsibility and we are committed to partnering with you to help you successfully comply with the GDPR. Requirements such as greater data access and erasure rules, privacy by design, and data breach notification processes may mean changes for your organization. Therefore, it is important to understand your obligations related to the GDPR and get legal guidance on how you can help your organization become compliant.

FAQ

Q: Does the GDPR require EU personal data to stay within the EU?
A: No, the GDPR does not require EU personal data to stay in the EU. However, the GDPR does require that a valid transfer mechanism is in place to protect the data before it leaves the EU.

Q: Does processing EU personal data always require the data subject's consent?
A: No. Consent is only one of the legal bases that can be used for the processing of personal data. For example, personal data can also be processed:

- When necessary for the performance of a contract to which the data subject is a party;
- When an organization has a legal obligation to do so (such as the submission of employee data to a tax authority); and
- Under an organization's legitimate interests which may include commercial and marketing goals. The legitimate interest must not, however, override the data subject's rights and interests.

Q: Will the GDPR fines apply to small and medium-sized enterprises ("SMEs")?
A: Fines for violations or non-compliance with the GDPR will apply regardless of the size of the company. If you are an SME, you are, in principle, subject to the same level of fines as a large multinational organization.

Q: Will Brexit impact GDPR compliance for UK businesses?
A: No. The GDPR comes into effect before the UK officially leaves the European Union, which the UK government has announced will take place on 29th March 2019. If you're based in the UK or process personal data from the UK, this means that you'll need to become GDPR compliant before 25th May 2018.

Q: Do EU data subjects have an absolute right to have their personal data deleted upon request?
A: A data subject's right to have his or her data deleted is often referred to as "the right to be forgotten." However, the right to be forgotten is not an absolute right. It only applies in certain circumstances and is subject to limitations. This right will not apply, for example, if processing is needed to comply with a legal obligation or is processed in the public interest relating to health.