Apogee Corporation Ltd
Nimbus House
Liphook Way
20/20 Business Park
Maidstone
Kent ME16 0FZ

T 0345 300 99 55
F 0845 330 99 44

Apogeecorp.com

Apogee Corporation (UK) Limited – Preparations For GDPR Compliance Statement

10th April 2018

Apogee Corporation Ltd ("Apogee") is committed to ensuring that its data processing activities are compliant with all applicable legislative and regulatory requirements, including the existing Data Protection Act 1998 and the imminent General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

In respect of our data processing activities, Apogee acts as a "Data Controller" in the provision of Managed Services and Outsource Services.

Taking into account the nature, scope, context and purposes of processing as well as the risks of and consequences for the rights and freedoms of natural persons, we have planned and implemented a company-wide project of appropriate technical and organisational measures to ensure, and to be able to demonstrate that retention and processing is performed in accordance with GDPR requirements, including;

i. Maintaining a record of processing activities under our responsibility as a Data Controller.
ii. At the time when personal data is obtained, making available to the data subject information relating to the identity of Apogee as the Data Controller, the purposes of the processing, any intention to transfer personal data to a third country or international organisation, the period for which the personal data will be stored, the right to request from Apogee access to, or the rectification or erasure, or restriction of processing concerning their personal data or to object to processing as well as the right to data portability, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent.
iii. Methodologies and Mechanisms:
    a. To consider the impact and security of data processing within process and systems implementation and, or change.
    b. In the case of a personal data breach, Apogee can without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55 of GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority cannot be made within 72 hours, we shall provide explanatory reasons for the delay.
    c. By which requests to access, rectify, erase or restrict the processing of personal data can be made and responded to within the stipulated one month timeframe.

This project is planned to deliver Apogee's compliance with GDPR by 25th May 2018 and to ensure that ongoing management is transferred to business as usual activities.

APOGEE

Scope Of Preparations

Apogee is very active in GDPR readiness preparations. Like most organisations, data is vital to our operations and success; while we endeavour to limit the amount of personal information we collect and process, we are committed to ensuring we do the right thing for Apogee, our clients, our employees and the third parties we work with.

By understanding our responsibilities and the changes GDPR will bring, we have developed and established a project for compliance. Supported by the Executive Board of Directors we are focussed on ensuring all tasks are in play, that they continue to progress, and by 25th May 2018 can be evidenced to demonstrate compliance.

We know that complete GDPR compliance for Apogee can only be achieved through a collaborative and transparent approach across all of our data processing operations and by making our project inclusive of clients, employees, suppliers and business partners.

Our project is based around 4 main areas:

Discover Determine what information we hold and for what purposes

This includes creating a data catalogue which details all the systems and documents the business holds that contains Personally Identifiable Information (PII). The catalogue details the actual data that is held (i.e. name, phone number etc.) and whether this is passed to a 3rd Party.

Inform Inform our clients of what data we hold and what it is used for

This will be done in a variety of ways including an updated privacy and cookie policy, and amendments to client contracts to clearly state our policy on 'use of data'. The policies will also inform clients what information we hold and how they can conduct a subject access request.

Protect Ensure our data is protected

We are reviewing our security policy and ensuring the whole business is compliant with it. This will include managing access to shared drives, systems, firewalls and general security compliance.

Access Ensure access is managed effectively

This covers how clients can obtain and manage the data we hold. This includes the right of access, right of erasure, right to restrict processing and right to object.

In summary our activities for GDPR readiness have included the following:

Data Processing Catalogue

We have largely completed our data mapping exercise. We know what data we have, where it is held, how we access it, the classification of the data, records of sharing and how we obtain and collect the data originally.

To enforce what we already know, we will be completing Legitimate Interest Assessments (LIA's) against all data processing that is identified as being for Legitimate Interest.

Privacy Notices

We want clients to know when and how we collect their data and how we will use it and share it. To fulfil this, we are re-issuing our privacy notice(s) and the information contained within our contractual agreements.

Information Security

Apogee is accredited to both Cyber Essentials and Cyber Essentials Plus and is compliant with the NHS's Information Governance Toolkit version 14.1.

Led by our Information Security Lead, we are focussed on maintaining an Information Security Framework which encompasses all appropriate aspects.

This includes technical security measures (e.g. intrusion, detection, firewalls, monitoring), encryption of personal data, restricted access to personal data, protection of our physical premises and hard assets, maintaining security measures for our team members, disaster recovery and training across all departments.

Responding to Individual Complaints and Data Subject Access Requests (DSARs)

We already have a process for dealing with consumer and employee queries and Subject Access Requests (SARs). This is a requirement under the Data Protection Act, therefore we are confident in our processes, which subject amendment to accommodate the change in permissible response times from 40 days to 30 days will provide timely responses to all DSARs.

Data Privacy Breach Management

We have effective data privacy incident and breach guidelines, which we will continue to review and enhance as required.

APOGEE

Privacy Impact – Privacy by design

We understand that when we introduce new systems or processes, or change existing systems or processes the privacy and security of information may be compromised. To fully understand the effects of change within systems or processes we are introducing Privacy Impact Assessments (PIAs) within all future change management projects and programmes.

End of Life Hardware

In providing our services, we understand the possible security impacts that could be posed when clients return old printers, multifunctional devices or IT equipment for disposal. Apogee can provide secure data deletion, overwriting removal and return or the destruction any embedded hard drive (or similar) at the end of life and provide certification where applicable, helping clients protect their data and achieve compliance.

Continuous Review of ICO Guidance

Like many organisations, we base our approach to compliance on guidance issued by the ICO. We recognise we cannot wait until all guidance has been released to implement our GDPR program, so have been pragmatic, progressing with our plan.

We continue to review guidance as it becomes available or is revised by the ICO and will adjust our implementation if appropriate.

For More Information

Enquires relating to GDPR compliance should be made to: marketing@apogeecorp.com

Apogee Corporation (UK) Limited

10th April 2018