GDPR Statement

Document Version: 1.1

Last Revision: 06 Feb 2019

1 Introduction

The EU General Data Protection Regulation came into force on 25th May 2018 and this introduced new responsibilities, including the need to demonstrate compliance and more stringent enforcement than the current Data Protection Act requires.

This document provides a statement on PAV's GDPR position

2 GDPR Statement

PAV ensures that their processes, activities and contracts are designed to allow Pav and its customers to comply with GDPR. PAV does not explicitly meet the requirements as defined by GDPR Article 37 to require a Data Protection Officer (DPO) however due to our services being delivered under ISO 27001:2013 and IG Toolkit the mechanisms and processes are closely aligned so a DPO has been appointed. The DPO has responsibility for PAV's GDPR compliance.

PAV are continually building on their comprehensive existing security and Information Security Management Systems (ISMS) to ensure they have robust procedures to underpin the requirements of GDPR and other applicable legislation.

Data classification and data lifecycles within PAV will ensure that we manage our data to comply with GDPR and as well as other current applicable laws and regulations

2.2 General Compliance

PAV has a robust ISMS and as a result of our ISO 27001:2013 adoption efforts, our Data types, processing, controlling systems, retention periods, etc have all been defined as part of the standard. Following a comprehensive review of the GDPR regulation, it has been determined that PAV's compliance is achieved by extending and enhancing our current processes, polices, control documents and contracts to meet the additional GDPR article requirements.

2.3 PAV's Data Processor Compliance

In many areas the hosted services or Cloud services provided by PAV already conformed to GDPR. As a data processor, the company has undertaking risk assessments of the data types we hold and how these are managed. Policies such as incident response plans and backup data retention have been reviewed and updated where necessary.

All PAV data centres reside in the UK. The processing of data within our Cloud systems is block data i.e. encrypted backup and DR data which cannot be read by PAV staff; or virtual servers where PAV has no access to the data unless agreements are made. Due to the nature of our services we do not inspect or manipulate our customer's data so we have no knowledge of the data types, we

simply ensure that our robust procedures do not allow the data to be lost or accessed by unauthorised bodies.

2.4 PAV Data Controlling Compliance

Personal data provided to PAV as a controller is kept to the minimum required to provide the services, for example the personal data controlled by PAV will be limited to names, email address and business and personal phone numbers. This data is categorised and held with defined handling procedures and is not sold or given to any third parties other than legitimate legal requests such as law enforcement agencies.