Data Protection Policy

Introduction

This policy has been drafted in response to the provisions of the General Data Protection Regulation which will apply from 30th June 2019.

Key Principles

This policy relates to:

- Personal data held in respect of the employees of AMP Infrastructure Limited
- Personal data held in respect of the management services provided by AMP Infrastructure Limited
- Personal data held in respect of the stakeholders of RWF LIFT and Medway LIFT

Personal Data means *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person';*

Due to the nature of the business it transacts the levels of personal data held by the company are relatively low for the following reasons:

- AMP currently has fewer than 10 employees
- AMP does not hold any sensitive personal data in respect of any individuals racial or ethnic origin, political opinions, genetic data, religious beliefs or sexual orientation
- AMP does not have members of the public as direct customers on a level that requires AMP to hold their public customer database
- AMP does not deal specifically in the processing of personal data as part of its business
- AMP does not deal specifically in the collection of personal data as part of its business
- AMP does not hold financial details of individual stakeholders or the general public
- AMP does not have any international transactions

However, Amp Infrastructure Limited takes the identification, storage and protection of all data extremely seriously and this is underpinned by a key principle of securely deleting any and all personal data that is no longer relevant and required.

To support these tenets it has undertaken the following review and implemented the following measures.

Reviewed: 30th June 2019

Identification

AMP has undertaken an exercise to identify any personal data held and to either permanently delete this personal data as it is no longer relevant or implement a system where relevant personal data is clearly identified, demarcated and held with extra access security in a recognised place on the company server.

This has been done in respect of all company emails on the system and a full review of information held on the company server.

Where possible personal data should not be stored on the email server and should either be permanently deleted or be moved to the AMP server and held in an identified secure area in a timely manner.

Storage and Access

A full review of how AMP staff access the Tresorit server has been undertaken as part of drafting this policy. The following points have been agreed.

There are currently 9 active licences being used by AMP.

Seven of these licences are held on devices kept predominately at secure AMP premises in Tunbridge Wells. Where possible laptops should be held securely on AMP premises.

When any of these seven laptops are moved out of the office staff will ensure that they are kept with them at all times where possible.

One laptop is held permanently remotely from AMP office.

Emails are accessed by AMP employees in the office and on secure mobile phones only.

Mobile phones are accessed via secure codes operated by employees to mitigate the risk of a data breach. This risk is further ameliorated by minimum personal data being held on the email server due to measures taken in the Identification phase of this policy.

Electronic Personal Data

Personal data identified will be held in a clearly labelled folder based on either its relation to AMP, RWF or Medway.

Each of these three sections will be individually password protected with access restricted to named individuals.

These sections will be reviewed on a regular basis to ensure that data held is specifically required and relevant and if it is not the case this data will be permanently deleted.

Hard Copy Personal Data

Any personal data identified as being required and held in hard copy form is stored at AMP office in locked cabinets with the keys held securely.

A policy of shredding any business related hard copy documents as the means of disposal is in place.

AMP Contacts

A full review of hard drive data base contacts has been undertaken and any personal data has been removed from this data base.

Protection

AMP stores the majority of its assets in some alarmed and locked premises.

AMP servers are situated remotely within the EU and protected by Cloud based security.

All laptops have individual passwords to enable access to be secured.

Webroot Secure Anywhere is installed on all laptops held at the AMP offices.

In conjunction with our IT Service Provider Cloudsol we have undertaken a full review of systems security to ensure that overall risks of a data breach can be minimised.

AMP Infrastructure Limited : Response to a Breach

AMP Infrastructure Limited is committed to take all necessary steps to prevent a breach of personal data occurring.

However, any breach in respect of personal data that AMP Infrastructure Limited is responsible for will be dealt with in the following way:

- Reported to a director of the company and where relevant the board of the relevant LIFT organisation
- An Impact Assessment of the breach will be carried out
- The Individual suffering the breach and the Information Commissioner's Office will be informed with 72 hours of the breach occurring
- Swift measures will be taken to remedy the breach and make amends for any damage caused by the breach

Reviewed: 30th June 2019

AMP Infrastructure Limited: Response to an Access Request

- AMP Infrastructure Limited will respond promptly to access requests from data subjects,
- It will disclose within 1 month the data and the kind of information included in a privacy notice;
- The identity of the person making the request must be verified.

AMP Infrastructure Limited: Liaison with Subcontractors

AMP Infrastructure Limited will continue to review the GDPR policy of the Facilities Management provider, Rydon Maintenance Limited to determine the have relevant procedures in place for data protection, specifically the:

- use of CCTV at the LIFT Health Centres
- procedures operated via Help Desk reporting
- procedures operated when reporting of accidents
- procedures operated when reporting insurance claims

AMP Infrastructure Limited: AMP Employees

AMP Infrastructure does hold the most personal data in respect of its employees. It protects this data by

- Holding payroll related data securely and separately in its data base
- Holding hard copy records in locked cabinets

AMP Infrastructure Limited: GDPR Policy - Review

This policy is ongoing and needs to be updated constantly to react to any potential threats that arise.

In addition, it will be subject to a formal review every 12 months.

The next date for review is 30th June 2020