GDPR Data Storage Policy

Who We Are (The Company)

APG Cover is a trading style of Future 45 Limited (The Company)

ADDRESS ..... The Business & Technology Centre, Stevenage SG1 2DX
COMPANY REGISTRATION No 5407413
DATA PROTECTION REGISTER No. Z933878X
FINANCIAL CONDUCT AUTHORITY (FCA) No. 461102
0208 543 6006
email@apgcover.co.uk

Why This Policy Exists

Your security comes first in everything we do. If your data is not secure, it is not private. This data storage policy ensures The Company:

Complies with data protection law and follow good practice
Protects the rights of customers, suppliers, business contacts, employees and other people The Company has a relationship with.
Is open about how it stores personal data
Protects itself from the risks of a data breach

Policy Scope

This policy applies to:

All data The Company holds relating to identifiable individuals, even if that information technically falls outside Data Protection Act 1998.
All customers, suppliers, business contacts, employees and other people The Company has a relationship with or may need to contact.

How And Where Is The Data Stored

From our bespoke data administration system to secure and reliable cloud infrastructures, the collecting, using, disclosing, retaining and disposing of data is secure and protected 24/7

APG Cover bespoke MSSQL DB Server data administration system. Password protected, 2048 Bit Industry Standard SSL Certificate issued by Trustico® a world leading SSL Certificate Provider. To provide maximum security the data centre is located in the UK within a secure compound consisting of perimiter fencing, electric gate entry and a gate house which is manned 24x7x365 by security personnel. Strict access controls are operational within the data centre building including proximity access card readers and secure lockable racks to prevent unauthorised access to the data centre and equipment. Backup data is stored in the UK, accessible only by engineers - ISO27001 accredited in terms of information security.

Data storage 1 meets and supports some of the highest benchmarks for security and privacy including ISO 27001, ISO 27018, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the BSI C5 attestation. With Binding Corporate Rules, C5 and the TCDP, Box has been independently reviewed for its privacy and cloud data protection.

Data storage 2 provides 24-hour monitoring of datacenters. Multi-factor authentication, including biometric scanning for datacenter access. Internal datacenter network is segregated from the external network. Role separation renders location of specific customer data unintelligible to the personnel that have physical access. Faulty drives and hardware are demagnetized and destroyed.

CRM complies with very strict security policies including hosted at Tier III+ or IV or PCI DSS, SSAE-16, or ISO 27001 compliant facilities

Secure dialler services provide state of the art data centres and servers, call recording complies with PCI Compliant Payments in Calls, information is kept confidential and stored safely, under strictly regulated conditions in accordance with the provisions of The Data Protection Act 1998.

Opayo payment service provider (PSP) meets has the highest level (Level 1) of the Payment Card Industry Data Security Standards (PCI DSS) certification to help protect businesses and shoppers from data theft and fraud. The Company never store your credit or debit card details

Our email marketing platform is hosted on servers in a UK based secure Tier III data centre facility. Access to the site is through a security 'airlock' and requires government issued photo identification. The entire site is covered by CCTV and monitored 24/7/365. All servers sit behind custom built firewalls which prevent unauthorised access and ensure data movement between servers occurs on a private network not accessible to the Internet. Database engines are not directly connected to the internet. A copy of the Pulsant Ltd DataCentre ISO27001:2013 Certificate of Registration is available on request. Data exchanged between our hosting environment and other systems (including platform users) is protected by 128 bit SSL encryption, preventing password and data snooping over the Internet. They do not rent, sell or otherwise disclose data to 3rd parties unless we are required to by law.

Email encryption. Where it is necessary to email sensitive data outside of our bespoke data administration system, messages and attachments are encrypted in a 256-bit AES-encrypted PDF wrapper and delivered directly into the recipient's inbox. Password protected and can be configured to send by transport layer security (TLS) automatically when TLS is detected and supported by both sender and recipient mail servers. Provides a Registered Receipt™ record detailing delivery status, time of delivery, and exact message content. This serves as court-admissible certified proof of delivery and can prove your compliance with privacy laws such as HIPAA.

More Information

If you're looking for more information, please let us know by contacting our Data Protection officer by telephone, email or post. All contact details are available at the top of this document.