GDPR Data Protection Policy

Introduction

The Company needs to gather and use certain information about individuals including customers, suppliers, business contacts, employees and other people The Company has a relationship with or may need to contact. This policy sets out their rights, our obligations regarding data protection, describes how Personal Data will be collected, handled and stored to meet the General Data Protection Regulations and to comply with the law.

The GDPR controls how your personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is used fairly and lawfully.

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that Personal Data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Definitions used by The Company (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of Personal Data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of Personal Data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the Personal Data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process Personal Data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

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

This data protection policy ensures The Company:

Complies with data protection law and follows 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 and processes individuals' 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.

Definitions

Personal Data

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.

Data Controller

The Company is the 'Data Controller' under the terms of GDPR legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The Company appoints a Data Protection Officer (DPO), who is available to address any concerns regarding the data held by The Company and how it is processed, held and used.

Data subject

Any living individual who is the subject of Personal Data held by an organisation.

Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data breach

A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. There is an obligation on the Data Controller to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the data subject.

Data subject consent

Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data.

Third party

A natural or legal person, public authority, agency or body other than the data subject, Data Controller, processor and persons who, under the direct authority of the Data Controller or processor, are authorised to process Personal Data.

Filing system

Any structured set of Personal Data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

The Personal Data We Need

Customer Data:

All Personal Data we collect is provided directly by you, and we only need the most basic personal information, which does not include any special types of information. We never collect personal information about you from other companies and will not share your information for marketing purposes with any third-party companies. You have the option to withhold personal information that is not required for the order process

Information we need to identify your quotation.

- name
- e-mail
- telephone

Additional information we need to issue a policy

- your address
- vehicle details

Current And Former Employees:

Personal Data held is required for administering Payroll under HMRC requirements, in line with employment contract, and also for daily staff management, no sensitive Personal Data is held. Recruitment data, held for a brief period of time to facilitate recruitment process.

Supplier And Client Data:

Basic, necessary data held for daily administration and the provision of the software and/or service.

Data Protection Law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The Data Protection Act is underpinned by eight important principles. These say that Personal Data must be:

1. Processed fairly and lawfully
2. Obtained only for specific, lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Data Protection Risks

This policy is designed to protect against very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately.
Failing to offer choice. For instance, all individuals should be free to choose how The Company uses their Personal Data.
Reputational damage. For instance, The Company could suffer if hackers successfully gained access to sensitive data.

Data Protection Officer (DPO)

Everyone who works for or with The Company has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles Personal Data must ensure it is handled and processed in line with The Companies GDPR data protection policies and principles. The Company is ultimately responsible for ensuring it meets its legal obligations.

The GDPR APG COVER Data Protection Officer Policy identifies the responsibilities of the DPO, contact information and should be consulted in conjunction with this Data Protection Policy

General Staff Guidelines

The Company provide training to all employees to help them understand their responsibilities when handling any data and in particular Personal Data. The only people able to access data covered by this policy should be those who need it for their work and should not share Personal Data informally.

When access to confidential information is required, employees can request it from their line managers.
Employees should keep all data secure by taking sensible precautions and following the guidelines set out in The Companies GDPR policies. In particular, strong passwords must be used and never be shared. Personal Data should not be disclosed to unauthorised people, either within The Company or externally. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

The GDPR APG COVER Data Storage Policy should be consulted in conjunction with this Data Protection Policy.
The following rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer.

When data is stored on paper, it is kept in a secure place where unauthorised people cannot see it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
When not required, the paper or files should be kept in a locked drawer or filing cabinet.
Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
Data printouts should be shredded and disposed of securely when no longer required.
When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
Data should be protected by strong passwords that are changed regularly and never shared between employees.
If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
Servers containing Personal Data should be sited in a secure location, away from general office space.
Data should be backed up frequently. Those backups should be tested regularly, in line with The Company's standard backup procedures.
Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

When Personal Data is accessed and used, it can be at the greatest risk of loss, corruption or theft. Therefore, when working with Personal Data, employees should ensure:

The screens of their computers are always locked when left unattended.
Personal Data should not be shared informally. In particular, if it is necessary to send Personal Data by email, data must be encrypted before being transferred electronically. The Data Protection Officer can explain how to send data to authorised external contacts.
Personal Data should never be transferred outside of the European Economic Area.
Employees should not save copies of Personal Data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires The Company to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the Personal Data is accurate, the greater the effort The Company should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
The Company will make it easy for data subjects to update the information The Company holds about them.
Data should be updated as inaccuracies are discovered.

Disclosing Data For Other Reasons

In certain circumstances, the Data Protection Act allows Personal Data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, The Company will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the board and from The Company's legal advisers where necessary.

Providing Information

The Company aims to ensure that individuals are aware that their data is being processed, and that they understand:

How the data is being used
How to exercise their rights

To these ends, The Company has a Privacy Policy setting out how data relating to individuals is used by The Company. The APG COVER Privacy Policy should be consulted in conjunction with the Data Protection Policy.

Data Protection Principles

The Company aims to ensure compliance with the GDPR by following the principles with which any party handling Personal Data must comply. This includes:

a) processed lawfully, fairly and in a transparent manner in relation to individuals.
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes.
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The Data Controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Lawful, Fair and Transparent Data Processing

GDPR ensures Personal Data is processed lawfully, fairly and transparently, without adversely affecting the data subject's rights. To ensure fair and transparent data processing we must be open and honest about our identity and how we intend to use and handle any Personal Data we collect about you (unless this is obvious) in ways you would reasonably expect. Above all, we will not use information in ways that unjustifiably have a negative effect on the data subjects.

Data processing will be classed as lawful if one of the following applies:

Consent..... The individual has given clear consent for you to process their Personal Data for a specific purpose.
Contract..... The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal obligation..... The processing is necessary for you to comply with the law (not including contractual obligations).
Vital interests ..... The processing is necessary to protect someone's life.
Public task ..... The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate interests..... The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests. The concept of legitimate interests as a lawful basis for processing is based on 3 key principles: Purpose, Necessity and Balancing.

What We Do With Your Data

We only collect the data required to provide our services and it is used for administrative, operational and marketing purposes and to communicate with you about your use of the services any changes to the services.

We will only pass on your information to other companies if it is necessary to perform our services.

Any personal information that you choose to provide to us or to other companies using our services will only be used in support of the intended purposes stated at the time at which it was collected and subject to any preferences indicated by you.

We only process Personal Data for the specific purposes set out in this policy (or for other purposes expressly permitted by GDPR).

Personal Data Retention

We will keep your personal information for as long as you are a customer of APG COVER. After you stop being a customer, we may keep your data securely stored for one of these reasons:

To respond to any questions or complaints.
To show that we treated you fairly.
To maintain records according to rules that apply to us.

Your information we use for marketing purposes will be kept with us until you notify us that you no longer wish to receive this information. More information on our retention schedule can be found on our web sites.

In all cases we will make sure that your privacy is protected.

The Rights of Individuals

GDPR defines the following rights to individuals:

a) The right of access to a copy of the information comprised in their Personal Data.
b) A right to object to processing that is likely to cause or is causing damage or distress.
c) A right to prevent processing for direct marketing.
d) A right to object to decisions being taken by automated means.
e) A right in certain circumstances to have inaccurate Personal Data rectified, blocked, erased or destroyed.
f) A right to claim compensation for damages caused by a breach of the Act.

Secure Processing

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. As detailed in this policy.

Accountability

Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances.
The accountability principle requires we demonstrate compliance with the principles and states explicitly that this is our responsibility.

To demonstrate accountability we will:

a) Implement appropriate technical and organisational measures to ensure and demonstrate compliance. Including internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
b) We will maintain relevant documentation on processing activities.
c) We have appointed a data protection officer, the Data Protection Officer Policy should be consulted in conjunction with this document.
d) We have implemented documentation that meets the principles of data protection by design and data protection by default.
e) We will provide details on Personal Data, how it is used and shared to the data subject
f) We will also create and improve security features on an ongoing basis. Following approved codes of conduct and/or certification schemes where appropriate.

Data Protection Impact Assessment

Data protection impact assessments will also be implemented where appropriate, they will be overseen by the DPO.
We will ensure they are used when using new technologies and if the processing is likely to result in a high risk to the rights and freedoms of individuals. The Data Protection Impact Assessment Principles should be consulted in conjunction with the Data Protection Policy

Right To Be Informed

Under the GDPR, each individual has the right to be given information about how their data is being processed and why. Our policies and web site explain how your Personal Data is being used at every step of the way and every effort is made to ensure the information we supply to you is concise, intelligible, easily accessible, free of charge and written in plain language.
There are a variety of categories of information including

a) Our identity and contact details
b) Identity of the data protection officer.
c) The purpose of the processing and the lawful basis for the processing.
d) Our legitimate interests.
e) Details of any recipient of the Personal Data.
f) Retention period or criteria used to determine the retention period
g) The existence of each of data subject's rights
h) The right to withdraw consent at any time, where relevant
i) The right to lodge a complaint with a supervisory authority
j) Whether the provision of Personal Data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the Personal Data

Right of Access - Subject Access Requests (SAR)

GDPR APG COVER SAR Policy should be consulted in conjunction with this Data Protection Policy. All individuals who are the subject of Personal Data held by The Company are entitled to:

Ask what information The Company holds about them and why.
Ask how to gain access to it.
Be informed how to keep it up to date.
Be informed how The Company is meeting its data protection obligations.

If an individual contacts The Company requesting this information, it is called a subject access request. If you would like a copy of the personal information we hold, please refer to the GDPR APG COVER SAR Policy and send your request to our DSAR Unit by telephone, email or post. All contact details are available at the top of this document. The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Right to Rectification

Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete. Response must be within one month. This can be extended by two months where the request for rectification is complex. Where we are not taking action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to Erasure

This is also known as 'the right to be forgotten'. It does not provide an absolute 'right to be forgotten'. Individuals have a right to have Personal Data erased and to prevent processing in specific circumstances. If a data subject requests the right to be forgotten, we must comply in the following situations:

a) Where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected/processed.
b) When the individual withdraws consent.
c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
d) The Personal Data was unlawfully processed (ie otherwise in breach of the GDPR).
e) The Personal Data has to be erased in order to comply with a legal obligation.
f) The Personal Data is processed in relation to the offer of information society services to a child.
g) Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

We can refuse to comply with a request for erasure where the Personal Data is processed for the following reasons:

a) To exercise the right of freedom of expression and information.
b) To comply with a legal obligation for the performance of a public interest task or exercise of official authority or the exercise or defence of legal claims.
c) For public health purposes in the public interest.
d) For archiving purposes in the public interest, scientific research historical research or statistical purposes

Right to Restrict Personal Data Processing

Where an individual contests the accuracy of the Personal Data, or has objected to the processing we will restrict the processing until you have verified the accuracy of the Personal Data.
When processing is deemed unlawful and the individual opposes erasure and requests restriction instead.
If we no longer need the Personal Data but the individual requires the data to establish, exercise or defend a legal claim.
Where these requests are made, we will only retain the Personal Data necessary and no further processing will take place.
Any Personal Data disclosed to third parties, will be informed about the restriction on the processing of the Personal Data, unless it is impossible or involves disproportionate effort to do so.

Right to Data Portability

The right to data portability only applies to Personal Data an individual has provided to the Date Controller, or where the processing is based on the individual's consent or for the performance of a contract and when processing is carried out by automated means.

We will provide the Personal Data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data.

If the Personal Data concerns more than one individual, we cannot provide the data on other individuals without their prior consent. We will respond without undue delay, and within one month. This can be extended by two months where the request is complex or we receive a number of requests.

We must inform the individual within one month of the receipt of the request and explain why the extension is necessary. Where we are not taking action in response to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Where data subjects have given their consent to process their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between us and the data subject, data subjects have the legal right under the Regulation to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other Data Controllers, e.g. other organisations).

Right to Object to Data Processing

You have the right to object to our use of your personal information, or to ask us to delete, remove, or stop using your personal information if there is no need for us to keep it. This is known as the 'right to object' and 'right to erasure', or the 'right to be forgotten'. Full details are provided in the Privacy Policy.

Security Data Breach Notifications

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing Personal Data. A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. All Personal Data breaches must be reported immediately to The Company's data protection officer.

On becoming aware of a breach, we will try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

If a Personal Data breach occurs, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will report it to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we will give reasons for the delay.

When reporting a breach, the GDPR says we must provide:

a description of the nature of the Personal Data breach including, where possible:
the categories and approximate number of individuals concerned; and
the categories and approximate number of Personal Data records concerned;
the name and contact details of the data protection officer
a description of the likely consequences of the Personal Data breach
a description of the measures taken, or proposed to be taken, to deal with the Personal Data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If it is unlikely there is a risk to people's rights and freedoms, it will not be reported to the ICO and we will document it.

Some Personal Data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose Personal Data has been compromised, therefore we will assess case by case, looking at all relevant factors.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly and without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, we will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If we decide not to notify individuals, we will still notify the ICO within 72 hours after having become aware of it unless it is demonstrated the breach is unlikely to result in a risk to rights and freedoms. In any event, we will document our decision-making process in line with the requirements of the accountability principle.

When notifying individuals we will describe, in clear and plain language, the nature of the Personal Data breach and, at least:

the name and contact details of the data protection officer.
a description of the likely consequences of the Personal Data breach; and
a description of the measures taken, or proposed to be taken, to deal with the Personal Data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Further details of notification procedure can be found in the APG COVER GDPR ICO Security Breach Notification Policy Document.

Procedure For Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests can be found on the ICO's website (www.ico.gov.uk) which provides

If you have any questions, please do not hesitate to contact The Data Protection Officer (DPO).

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.