General Data Protection Regulation (GDPR) Policy

Overview

The Excalibur Group is fully committed to compliance with the requirements of the General Data Protection Regulation. The Excalibur Group will therefore follow procedures which aim to ensure that all personnel with access to any personal data held by the Company are fully aware of and abide by their duties under these regulations.

The Excalibur Group holds personal data about partners, customers, suppliers and other individuals for a variety of business purposes.

The Excalibur Group has a commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

Definitions

Partner	An Excalibur Employee
Business purposes	Using your personal information We may use and analyse your information to: • Process the goods and services purchased from us and to keep you updated during the ordering process • Bill you for using our products and services • Carry out a credit check if you're applying for a contract or credit through us or third party to assess your application • Keep you informed generally about new products and services we provide (unless you opted not receive our marketing messages and newsletters) • Respond to any questions or concerns you may have about our services • Prevent and detect fraud or other crimes, recover debts or trace those who owe us money • Provide information to our partnered third parties to fulfil your purchase or contract. • To inform you of interruptions to any services we supply • To provide details business analysis as part of your service reviews, this maybe via our 3rd party vendor who is GDPR compliant • If you are subscribed to monitoring tools such as GFI or MDM services which are linked to user names and can be monitored for but not limited to, the following purposes dependant on the monitoring tools you've opted for as part of your service agreement: - o Asset management o Hardware health check o Hardware software log o Back-up tracking and Disk health o Patch management o Web monitoring o Data usage o Location tracking At Excalibur we don't use, store or analyse this data for behavioural tracking. We only apply the tools/applications requested and set out in the service agreements you hold with us. If you use this data for behavioural monitoring or tracking within your company, you should make your staff aware of such within your handbook policies.
Personal data	'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. *Personal data we gather may include: individuals' phone number, address, email addresses, job title, financial and payment details, online portal access details, server passwords and user logins for remote support.*
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processing	'Processing' means 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.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for The Excalibur Group is the Information Commissioners Office (ICO).
High Risk Breach	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.

The Principles

The Excalibur Group shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in what we do to comply with these principles. The Principles are:

1) Lawful, fair and transparent - Data collection must be fair, for a legal purpose and we must be open and transparent about how the data will be used.
2) Limited for its purpose - Data can only be collected for a specific purpose.
3) Data minimisation - Any data collected must be necessary and not excessive for its purpose.
4) Accurate - The data we hold must be accurate and kept up to date.
5) Retention - We cannot store data longer than necessary.
6) Integrity and confidentiality - The data we hold must be kept safe and secure.

Accountability and transparency

We will ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. Excalibur are responsible for keeping a written record of how all data processing activities, and ensuring we comply with Principles listed in the previous section of this document.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. We are responsible for understanding the responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up-to-date and relevant documentation on all processing activities
- Providing GDPR training and awareness to all employees within the Excalibur Group
- Logging any data breaches
- Continual data cleansing and disposal through secure means
- Provide our customers with a clear and easy data withdrawal process
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Transparency
    - All Excalibur devices are registered and managed via an Endpoint Management solution.
    - Automatic device locking
    - All Excalibur laptops have been encrypted using Microsoft Bitlocker software
    - All Excalibur employees content stored onto OneDrive, meaning this is stored on our cloud and in the event of a device being stolen or breaking we can retrieve your data
    - Excalibur have reviewed all internal policies to ensure they keep data protection at highest priority and full in line with GDPR regulations
    - Excalibur hold the Cyber Essentials and ISO:9001 certification and maintain an efficient QMS resulting in employees always following best practice

Our Procedures

Fair and lawful processing

We will process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

The Excalibur Group Leadership team are classified as data controllers and have been given relevant training in GDPR. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling data. We will log all data breaches to the ICO within the timeframe specified and hold such detail on a data breach register for future reference.

Data processors must comply with our contractual obligations and act only on the documented instructions of the data controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the leadership team. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent -** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract -** The processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation -** We have a legal obligation to process the data (excluding a contract).
4. **Vital interests -** Processing the data is necessary to protect a person's life or in a medical situation.
5. **Public function -** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. **Legitimate interest -** The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform your Manager.

Data security

You will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Manager responsible will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly. We encourage all partners to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used
- The Operations Director will approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data will be regularly backed up in line with the company's backup procedures
- Data will never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data will be approved and protected by security software

Data retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Rights of individuals

Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This will be done without delay, and no later than one month. This can be extended to two months with permission from Management.

4. Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We will retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We will respect the rights of individuals in relation to automated decision making and profiling.

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed. To submit a 'subject access request' please complete the form located at https://www.excaliburcomms.co.uk/wp-content/uploads/SUBJECT-ACCESS-REQUEST-FORM.pdf and send it to GDPR@excaliburcomms.co.uk.

How we deal with subject access requests

We will provide an individual with a copy of the information requested, free of charge. This must occur without delay, and within one calendar month of receipt. We will endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible.

If complying with the request is complex or numerous, the deadline can be extended to two months, but we will inform the individual within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed;
- Where consent is withdrawn;
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation; or
- The processing of personal data to offer information society services to a child.

How we deal with the right to erasure

We will only refuse to comply with a right to erasure in the following circumstances:

- Whereby we need to use the data to service your contractual agreement
- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

If we have disclosed your personal data to any of our 3rd party suppliers to provide the services obtain through us, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked, we must inform you of those suppliers.

To submit a 'Data Subject Consent Withdrawal' please complete the form located at https://www.excaliburcomms.co.uk/wp-content/uploads/DATA-SUBJECT-CONSENT-WITHDRAWAL-FORM.pdf and send it to GDPR@excaliburcomms.co.uk.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

We must cease processing:

- For direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- We must deal with an objection to processing for any direct marketing at any time, free of charge

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

Third parties

Using third party controllers and processors

We will have written confirmation from any third-party data processors that we use.

We will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts
Our contracts will comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available.

We will only rely on Contract as a lawful basis if we need to process your personal data:

- To fulfil a contractual obligation to you; or
- Because you have asked us to do something before entering into a contract (e.g. providing a quote); and
- The processing is necessary.
  If we can reasonably do what is required without processing personal data, this basis would not apply.

Data audits
We will conduct regular data audits to manage and mitigate risks, which will be held on a data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches
As soon as Excalibur Communications become aware of any breach we have a legal obligation to report the data breach to the ICO within 72 hours, where feasible and if a high risk breach, inform the individual effected and the action plan we are putting in place to rectify such.

All our Employees have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any employee who fails to notify of a breaches, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.