# The Barkby Group PLC Documentation

The General Data Protection Regulation (GDPR) comes into effect on the 25th May 2018, replacing the Data Protection Act 1998 (DPA). The principles of GDPR are similar to the DPA, but with added detail, particularly on accountability (where the organisation must show how you comply with the principles of the regulation).

As a data processor, The Barkby Group must abide by the GDPR or risk facing administrative fines. This means that a review of all data processing must be completed in order to establish the lawful basis for processing any Personal Data or Sensitive Personal Data, whether digitally or by manual filing methods.

Data Protection covers the processing of personal data, which can be any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, postal address, bank details, posts on social networking websites, medical information, or a computer IP address.

The business must also prove how data outside the scope of GDPR is anonymised or is not defined as personal data.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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 in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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 in the public interest, scientific or historical research purposes or statistical 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;
- 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.

Key areas for our business can be summarised as:

- Lawful Processing – we must legally justify every single process that involves data within the business and record this. A large proportion is likely to be able to be justified as 'Legitimate Business Interests' but it must be proven why.
- Consent – where 'consent' is our legal justification for processing data (one of the eight legal justification options), we must ensure the consent we gain is compliant with the new regulations, especially around Fundraising, and that we employ appropriate retention processes of consent and allow people to change their consent.
- Data Erasure – we must allow data subjects to 'erase' their data, and define exactly what that means for our systems.
- Profiling – we must review how we profile customers or donors and ensure we are compliant with the new regulations.

- Data Breach Notifications – should a data breach occur (either digitally or physically) we must report this breach
- Demonstration of Compliance – we must have a rigorous system which documents our processes, justifications, and safeguards of compliance, which can be shared as evidence and scrutinised by the ICO in the event of any data protection investigations.

Scope
This policy applies to all staff. You must be familiar with this policy and comply with its terms.
This policy supplements our other policies relating to internet and email use.

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

Our Responsibilities
General:

- Keeping the company updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Fosters
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

IT:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Marketing:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Sensitive personal data
The data we collect is subject to active consent by the data subject, unless we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

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.
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 should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention
We must 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.

Data portability
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Data audit and register
Regular data audits to manage and mitigate risks will inform the 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
All members of staff 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 Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring
Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

## Privacy Policy

The GDPR is a comprehensive data protection law that replaces existing European privacy laws and strengthens the protection of personal data in an increasingly data driven world. The GDPR

is enforceable in each EU member state and gives individuals greater control over their personal data. It comes into effect on 25 May 2018.

What we collect

We ask for your name, address and contact details when you book a restaurant reservation or a room with The Barkby Group PLC. This enables us to communicate with you regarding the details of your event/stay/reservation, but also fulfils our legal obligations for invoicing.

How we store the information

We take great care to keep your personal information safe, The Barkby Group PLC databases are kept partly on a secure physical server within our locked offices, and partly on the cloud run by Microsoft Azure. Both areas have restricted access with numerous levels of security to prevent unauthorised access to those servers including firewalls and passwords.

What we do with the information

The primary use of the data we collect is to communicate with you to provide your event service.

Who we share the information with

We do not share your information

Retention and Destruction

Our policy is to provide our customers with control over retention and destruction of their data. Customer accounts can be deleted anytime. Deletion from our customer database is instant and irrecoverable, but deletion from accounts databases has to comply with HMRC legislation. Any data stored on backups will be deleted entirely within 7 days.

What we don't and won't ever do

We don't, and never will sell or rent your information to any 3rd party.

The Barkby Group PLC full GDPR documentation and personal data registry audit is available on request.

# Personal Data Registry

| System | Collected By | Data Collected | Data use | Shared with | Stored | Cleansed |
|---|---|---|---|---|---|---|
| Goldmine & Quotewerks | Sales & Marketing- provided by client | Name, phone number, email address | To provide quote/ services to client | Venue | Physical server @ Feeder Road | 3 years |
| Mail Chimp | Sales & Marketing- provided by client | Name, phone number, email address | Marketing | The Barkby Group PLC staff only | | |
| Sage Line 50- client data | Accounts- provided by Sales Team and/ or client directly | Name, email address, postal address (for HMRC complaint VAT invoice). | To provide quote/ services to client | Client only | Physical server @ Feeder Road | 7 years to be compliant with VAT legislation |
| Sage Line 50- supplier data | Accounts- provided by supplier | Names, phone number, email address, key contact details, bank details | To process suppliers invoices and pay for goods/ services provided | Client only | Physical server @ Feeder Road | 7 years to be compliant with VAT legislation |
| RBS Bank Online | Accounts- information provided by employee or supplier | Suppliers and staff sort code and account number | To pay suppliers/ staff | N/A | Online system with 4 stage password entry and Trusteer Rapport Antivirus software | Details are removed once we know we are not using the supplier or employing the staff member anymore. |
| Xero payroll | Accounts- information provided explicitly by employee | Name, address, DOB, NI number, tax code, hours worked, salary £, | To process payroll, RTI returns, calculate pension and holiday allowances. | Employees only | Physical server @ Feeder Road | Annually, staff are P45'd off at the end of each fiscal year. Staff are archived |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | email address and bank details. | | | | but not removed. |
| B&CE pensions website | Accounts- information provided explicitly by employee | Name, address, DOB, NI number, tax code, hours worked, salary £. | To process pension contributions in line with automatic enrolment requirements | B&CE pensions only | Online system with 4 stage password entry | Staff details are removed from the system once we know they are no longer employed by The Barkby Group PLC |
| Staff phones | Individual staff members | Name, phone number | To communicate re events | N/A | On individual phones, no server not shared; required pin entry | |
| ResDairy database | Sales & Marketing- provided by client | Name, phone number, email address | To provide quote/ services to client | N/A | Physical server @ Feeder Road | 3 years |
| Dropbox | | | | | | |
| Canada Life | Accounts | Selected staff details only | To enable life insurance | Canada Life | Excel on The Barkby Group PLC server | Revised annually |
| Aviva Healthcare | Accounts | Selected staff details only | To enable private healthcare | Aviva Healthcare | Email | Revised annually |
| Retail Merchant Services | Accounts | Card payment details | To receive payment | FDMS | Not stored at all | N/A |