Policy title :	Data Protection Policy

AG Barr
BUILDING GREAT BRANDS

1. POLICY

Both you and the Company must comply with their obligations and responsibilities under the retained EU law version of the General Data Protection Regulation (EU) 2016/679 ("UK GDPR") and the Data Protection Act 2018 ("the Acts") in respect of personal data.

We are committed to respecting personal data and processing it in an open and fair manner. Equally, we expect our employees to comply with the Acts and the importance of respecting people's privacy rights. Whenever you are working with data relating to individuals you should always have data protection at the forefront of your thinking and any projects should be data protection compliant by design. If you are ever unsure of whether or not something is compliant or if you feel you require more training on data protection then you should contact the legal team at dataprotection@agbarr.co.uk.

This policy will help give you guidance on how the Company aims to achieve our objectives of processing personal data in a secure, open and fair manner and what is expected of you in order to help us meet these objectives.

2. TERMINOLOGY & PRINCIPLES

We are committed to complying with the "data protection principles" in relation to all personal data that we process.

"Personal data" is data which relates to a living individual who can be identified from that data. It can be factual (e.g. name, address or date of birth) or it can be an opinion (e.g. performance appraisal).

"Processing" personal data means obtaining, holding, organising, using, disclosing, manipulating or destroying it - in fact, doing almost anything that one can do with information.

According to the data protection principles, all personal data should:

(i) be processed fairly and lawfully;

(ii) be obtained only for one or more specified purpose(s) and should not be used for other purposes;

(iii) adequate, relevant and not be excessive in relation to the purpose for which it is processed;

(iv) be accurate and kept up to date;

(v) not be kept longer than is necessary for the purpose for which it is processed; and

(vi) be processed in a manner that ensures appropriate security of the personal data.

3. SCOPE AND COVERAGE

Personal data processed by the Company will fall into the following principal categories:

3.1. Employee Information - information relating to directors, employees (permanent and temporary) and applicants for employment.

Examples of employee information held by the Company include name, address and contact details, attendance records, information on medical conditions, performance reviews, bank details (for payroll administration only) and salary information. It may also include information obtained from any monitoring activities (e.g. internet usage and email monitoring).

Some employee information held may be "special category personal data" under the Acts. Special category personal data is information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Special category personal data about employees will only be processed where this is necessary. You can review the HR tab of the Personal Data Register for more information about this (link).

3.2. Consumer and Customer Information - information relating to consumers, customers and contacts (to the extent that this relates to individuals only).

3.3. Supplier Information - information relating to suppliers (to the extent that this relates to individuals only).

Examples of customer information and supplier information held include the names, business phone numbers and e-mail addresses of individuals working for the customers/suppliers. Examples of consumer information include the names, phone numbers, postal addresses and e-mail addresses of individuals who enter brand prize draws, promotions and competitions.

4. OBTAINING AND USING PERSONAL DATA

4.1. Employees and Job Applicants

All personal employee information is obtained and held for the purposes of the relevant person's employment (or, in the case of applicants, potential employment). Such information should not be used by the Company for any other purpose without the employee's (or applicant's) consent.

We require applicants to complete standard application forms and new employees to complete "new starter" forms. These forms seek personal details about applicants and newly appointed employees. The purpose of these forms is to gain information which we consider necessary and appropriate to obtain for the purposes of employment or the consideration of employment.

The Company's internal-facing Employee Privacy Policy (available on the HR Portal) explains to employees how we collect, store, use, and process the personal data that an employee provides or that the Company collects. The Company's external-facing Recruitment Privacy Policy (available at www.agbarr.co.uk/termsofbusiness) explains how we collect, store, use and process the personal data a job applicant provides, or we collect, during the recruitment process. Data will only be used for the purposes set out in these policies. More information can be found in the Company Personal Data Register (link).

4.2. Consumers, Customers and Suppliers

Customer and supplier information may only be used for the purposes of supplying/ordering goods to/from them (as appropriate) or for the purposes of providing customers or suppliers with related information. Consumer information may only be used for the purpose for which it was gathered and as notified in detail to the consumer. No personal consumer, customer or supplier information should be used for any other purpose without the relevant individual's consent. The Company's external-facing Customer Privacy Notice and Supplier Privacy Notice can be found at www.agbarr.co.uk/termsofbusiness.

4.3. Using Personal Data

As well as following the above you should always consider whether or not the processing is fair to the individual affected. For example, the Acts specifically call out fully automated decisions about individuals as being unfair. You should therefore always ensure that any decisions about individuals have some form of human input.

It is important that we keep track of how we use personal data as a business. Before any new project or process type which involves personal data is to begin, or where an existing process is to be done with different technology, a personal data processing form must be completed (link) by the process/project owner. If the answers on the form indicate that the processing is high risk then you must not begin the processing until you have approval from the legal team. The form should be completed by the project/process owner.

When the legal team receives a data processing form with the processing risk marked as high, they should perform a privacy impact assessment. This assessment will review:

- Whether the proposed process complies with data protection requirements;
- Whether any additional safeguards need to be put in place to reduce any risks to the people whose data is being processed;
- If the regulator should be consulted/informed about the processing; and
- Whether any further steps are required in order to ensure the data is processed in a fair manner.

Once the legal team has conducted the privacy impact assessment they may either approve the processing (with any additional measures they think are necessary) or reject the proposed processing.

5. STORAGE OF INFORMATION

5.1. Employee Information

Information relating to employees of the Company must be kept on the dedicated HR platform. Managers and departments should not retain copies of this information unless it is absolutely necessary and the legal team is informed. Copies should not be held outwith the dedicated HR platform for any longer than is strictly necessary. Access to the HR platform should be limited to Managers, members of HR and only to such other employees as may be authorised in particular circumstances.

When any personal data is obtained from employees, applicants for employment or agency workers it should be passed to HR for storage in the relevant database.

No director, manager or employee should individually keep any personal data relating to any employee or potential employee (except for name, address and contact details), except where a director/manager/employee requires to use such records for specific employment purposes for a limited period, in which case they must be kept securely and only for so long as necessary for that purpose.

Further information on how employee information is stored and processed can be found in the Employee Privacy Policy (available on the HR Portal) and on the Personal Data Register (link).

5.2. Consumer/Customer/Supplier Information

This information will be held in individual employees' contact lists, paper files or in one of the following systems: Google Drive (with appropriate share settings), JDE, Van Sales, Mainsaver, payroll systems, CRM or Customer Care. This information must not be held in any other system and must not be held on USBs or laptops. The general security surrounding our IT systems will protect that information.

5.3. Personal Data

All personal data held by the Company should be stored securely and access should be restricted to those who need to use it.

As it is extremely difficult to keep track of the sharing settings and the deletion of documents on Google Drive, you should avoid storing documents which contain personal information on Google Drive except where this is unavoidable. In these instances you must exercise a great deal of care to ensure that the data is deleted when it is no longer needed for the purpose it was made (in line with our Personal Data Register - link) and that only those who require access to the data are shared on it.

Documents containing personal data which are shared on Google Drive should be shared with a relevant team using a Team Drive (link to guidance) rather than with the individual members of a team. This allows the permissions to be more easily managed when people leave the team and to keep track of who has access to documents.

6. DISCLOSURE OF PERSONAL DATA

It is important that the confidentiality of personal data is maintained insofar as possible but there will be scenarios in which personal data will be disclosed. In these scenarios, the guidelines set out in 6.1 and 6.2 should be followed. If you are the person disclosing personal data, it is your responsibility to ensure you comply with these requirements and if you are unsure of whether or not the disclosure is permitted then you should check with the legal team.

6.1. Employee Information

Only the employees noted in section 5.1 should have access to employee information, however:

all employees' business addresses and contact details are circulated within the Company and, to some extent, externally (e.g. on business cards, Google profiles and email auto-signatures)

employee information (including sensitive personal data) is disclosed to third parties for the purposes of employee benefits (e.g. administration of pensions, life assurance, share schemes etc) and other purposes set out in the Personal Data Register (HR tab). In particular, the trustees of the Company's pension schemes, or the administrators acting on their behalf, may transfer employee information (including sensitive personal data), outside the EEA for the purposes of the administration of the pension schemes and in connection with the trustees' use of the administrator's website.

If you object to such personal details being disclosed in any of these ways, please notify your Manager in the first instance.

Except as detailed above, we shall not disclose any personal information about you to any third party without your consent except:

- as may be required by law or for regulatory purposes;
- as requested by appropriate authorised, regulatory or governmental authorities, such as HM Revenue and Customs;
- as may otherwise be permitted under the Acts; or
- as set out in the Employee Privacy Policy (available on the HR Portal) and Personal Data Register (HR tab).

If disclosure of personal employee information is requested or required in other circumstances then, if the employee consents to the disclosure of his/her personal data, or if the legal team approves the disclosure then the disclosure may be made.

6.2 Consumer/Customer/Supplier Information

Personal consumer, customer and supplier information should not be disclosed to third parties without a data processing form (link) being completed by the project/process owner. The project/process owner should also contact the IT department to ascertain whether or not they require the third party to complete an IT Security Supplier Questionnaire.

Where personal consumer, customer or supplier information may be disclosed to a third party in one of the circumstances outlined above, it must only be disclosed under a written contract containing provisions designating the third party as a data processor and requiring that third party to comply with the obligations of a data processor under the Acts.

6.3 Transfer of Information

Where we are transferring personal data within our organisation or to others outside the organisation, we need to ensure that we transfer the information in a secure manner appropriate for the kind of information transferred. For example, it would be unacceptable to transfer bank details by post. Where particularly sensitive information (such as bank details or information about an employee's health) is being transferred, IT should be contacted to ensure appropriate safeguards are in place.

If you have a good reason to share/transfer personal data or confidential information externally, you should follow these Google Drive Sharing Tips which allow you to use the secure Google Drive features and controls such as setting expiry dates for access and preventing the ability to download documents (link).

7. ACCURACY OF PERSONAL DATA

7.1. Employee Information

The Company is responsible for ensuring, insofar as possible, that any personal data held is accurate and kept up to date.

Employees are responsible for advising the Company of any changes to their personal information.

The HR Department is responsible for ensuring that we check with employees regularly that their home address held is correct.

7.2. Consumer/Customer/Supplier Information

Consumers, customers and suppliers should be asked to advise the Company when any personal information that is being held becomes out of date. We have an obligation to rectify inaccurate personal information.

8. RETENTION, SECURITY & DESTRUCTION OF PERSONAL INFORMATION

Personal data of any kind should not be held for longer than is necessary for the purpose for which it was obtained or collected.

8.1. Personal Data Register

We maintain a Personal Data Register (link). This sets out in multiple tabs the personal data used, processed and collected by most functions within the Company. You should retain documents in line with the relevant stated retention periods and employees are responsible for ensuring documents and information they control are deleted in line with the periods set out in the policy unless there is a good reason why a specific document needs to be retained for longer than the allotted time. For a document to be deleted it needs to be non-recoverable electronically and all paper copies should be shredded or securely destroyed. If you cannot find a relevant retention period in the Personal Data Register or generally have any questions about the Personal Data Register please contact your Line Manager in the first instance. Alternatively you can contact the Data Guardian for your function (link) or email dataprotection@agbarr.co.uk.

8.2. Consumer/Customer/Supplier Information

To the extent that personal information about consumers or employees of customers/suppliers is kept on an employee's contact list, each employee is obliged only to retain such information for as long as the contact information remains relevant for the purpose it was collected or in line with the Personal Data Register.

8.3. Deletion of Emails

Emails can be difficult to manage and some employees can be inundated with hundreds of emails per day. However, often emails contain personal data meaning that they should be deleted as soon as they are no longer needed. Examples of personal data which could be contained in emails include things such as opinions about people (including employees), information about their health, political views, racial or ethnic origin, performance reviews, salaries, home address, bank details or any other information which specifically relates to a named person.

The following steps should be taken in order to help manage the deletion of emails containing personal data:

- You should set up a personal data folder on your Gmail account. This is done by clicking "more" on the left-hand column of your inbox and then selecting "Create new label". The new label should be named "personal data".
- File any emails you receive which contain personal data into this folder.
- Review the personal data folder regularly (at least once a month) and delete any emails once they are no longer required.

9. MINIMISATION OF PERSONAL DATA

The more personal information we hold about individuals, the greater the risk to them if a data breach occurs. You should only collect such information as is strictly necessary for the purpose for which you intend to use it. For example, if we are running an online competition it would not be necessary to collect the home address of each entrant.

In order to reduce the personal data we hold, wherever possible, information should be anonymised or pseudonymised. This may be appropriate where, for example, we are using the information for statistical purposes only and there is no need to link the information to identifiable individuals. Another example would be in conducting market research surveys. Whilst it may be necessary to collect information about a consumer for the purposes of identifying their demographic, there may not be a need to record their name.

10. MONITORING

The Company's "I.T. Acceptable Use Policy" (available on the HR Portal) sets out the policy on e-mail, internet and general system usage.

Information about internet usage by employees is monitored in certain circumstances. To the extent that this information is "personal data" within the meaning of the Acts, it must be processed in accordance with the data protection principles outlined in paragraph 2 of this policy.

CCTV and surveillance systems are used around the Company's premises and in all of the Company's vehicles for security and Health & Safety purposes. See paragraph 14 below for more information.

11. CHILDREN'S DATA

Under the Acts children receive an enhanced level of data protection. You should avoid collecting any personal information about children or directing any of our websites towards them without the specific approval of the legal team. Promotions and competitions should be open to ages 16+

only. If you believe that a project or scheme may inadvertently be collecting information about children then you should contact the legal team.

12. SUBJECT ACCESS REQUESTS

Under the Acts individuals have the right of access to information we hold which relates to them. This includes electronic and paper documents and email correspondence including where an opinion is being offered about the individual. A request for information by an individual is known as a subject access request (**"SAR"**).

12.1. Informing the legal team

Where you receive a subject access request, it should be sent to dataprotection@agbarr.co.uk. Often responding to a SAR can be time consuming and the Acts require us to respond within one month. It is therefore very important that the legal team is informed of the SAR as soon as possible. You should not respond to any written SARs without first consulting with the legal team but the legal team will require you to take responsibility for compiling the relevant information and responding to the individual. If necessary, the legal team will provide you with guidance on what information should be included.

12.2. Informal Requests

Occasionally you may also receive informal or verbal requests from individuals for certain information relating to them. Where the information set requested is not commercially sensitive, you are confident of the individual's identity and the information requested does not contain any information relating to any other individuals, then you may provide the information to the individual without the need to consult the legal team. Examples of where this would be acceptable include a request to know how many days annual leave entitlement an employee has or a former employee requesting a copy of their p45.

12.3. Responding to the Request

The Acts require that if the request is received in an electronic format (e.g. email) then we are required to respond in a suitable electronic format rather than in a letter. In all instances, including in response to informal but written requests, our template holding response letter (link) and substantive response letter (link) should be used to respond to the request. The holding response should be sent as soon as possible and the substantive response should be sent within 30 days of receipt of the request. You should inform the legal team if you think we will be unable to meet this timescale. The response letter should be reviewed by the legal team before the response is sent.

Where the request is made by someone with a disability you should consider whether an alternative format of response such as braille or audio would be appropriate.

12.4. Employee Requests

As well as consumers, suppliers and customers, employees are entitled to request and retain copies of information held about them.

Requests to access personal information should be made to your immediate manager in the first instance or to the legal team. All members of staff dealing with a request by another employee should inform the legal team of the request before formally responding. If an employee makes an informal, verbal request to see information about them then their manager may provide it without informing the legal team if the data does not include information about any third party, is not commercially sensitive and if it is appropriate for it to be disclosed.

12.5. Right to Object

Individuals have the right to object to the way we process their information and to have inaccurate information about them amended. Where you receive an objection or a request for the information we hold to be amended or deleted, you should inform the legal team who will provide you with assistance in responding and dealing with the request.

13. DETECTING SECURITY BREACHES

Our IT staff should keep appropriate measures in place to detect breaches of our security. However, all employees should also be vigilant of suspicious activity. Where you are aware of data potentially being accessed by unauthorised users or where data is lost, you must notify the IT department and the legal team as soon as possible along with our data breach response team at responseteam@AGBarr.co.uk.

14. CCTV

CCTV and surveillance systems are used around the Company's premises and in all of the Company's vehicles for security and Health & Safety purposes. To the extent such footage identifies an individual, this would be considered personal data under the Acts. Video footage is reviewed periodically for example to monitor Health & Safety practices or if there is a security issue or question of criminal activity. Video footage must be processed by the Company in accordance with the Acts and the Company CCTV Policy. Dependent on the specific recording system there is a regular process of overwriting old video footage. The Company may share CCTV footage with third parties in very limited circumstances.

The Company's CCTV Policy (available on the HR Portal) (link) contains detailed information on the Company's approach to such CCTV and surveillance systems. Retention periods (depending on the site) can also be found on the Personal Data Register (link).

15. CONTRACTS WITH DATA PROCESSORS

It is important that we effectively manage our relationships with those who process personal information on our behalf and we need to ensure that we have suitable data protection requirements in place when using third party processors. Contracts involving the processing or storage of personal data should always be referred to the legal team before they are agreed to. This includes where we are agreeing to the processors' standard terms for the first time.

16. BREACHES OF POLICY

You should only hold and use personal information in accordance with our policy and procedures and any such data should be kept up to date and accurate.

You should not disclose to any person any personal information about a consumer, customer, supplier, another employee, a director or any third party which you gain in the course of your employment, without specific authorisation from the Company or the relevant individual.

Failure to comply with any of this policy will be viewed seriously and may lead to disciplinary action being taken against you. Depending on the severity of the breach, this may be treated as gross misconduct and may result in your dismissal from the Company. You should also be aware that criminal liability arises from certain breaches of the Acts.

17. NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE

The Company has given notification to and registered with the Information Commissioner's Office. These notifications/registrations must be kept up to date and renewed regularly. The Company Secretarial Department is responsible for ensuring that this is done.

18. DIRECT MARKETING

Direct marketing is a frequently used marketing technique which involves contacting individuals directly with the purpose of making a sale. For the purposes of the Acts, direct marketing includes any marketing or sales correspondence sent directly to specific individuals. Examples of direct marketing include sending promotional texts and making sales calls to our customers.

Direct marketing is a heavily regulated area and breach of the rules can result in large fines. The Direct Marketing Guidelines (link) should be followed when conducting any direct marketing campaign.

19. RISK REGISTERS

It is important that data protection risks across the business are regularly reviewed. All departments should keep a risk register and data protection should be included in this register. The risks covered should include the general data protection risks (e.g. data breaches) and any risks which are more likely to affect specific departments. The heads of each department are responsible for ensuring data protection is included on the register.

20. DATA PROTECTION CHAMPIONS

Each department should have a data protection champion. The Data Guardian will be given more detailed training on data protection and should be your first point of contact should you have any queries. Their role will also involve offering advice to the department or the legal team on where there may be potential data protection issues. You can find the current list of Data Guardians here (link).

21. PHOTOGRAPHS OF STAFF

From time to time we may wish to feature photographs of our employees in internal or external publications (for example: our intranet, our corporate website or professional networks such as

LinkedIn). The Communications & Corporate Affairs team will always seek the permission of employees before publishing photos in external publications. Your photograph will also normally feature on your issued employee card for site security and identification purposes.

22. TRAINING AND QUESTIONS

The Company is committed to ensuring that all staff are aware of their obligations under the Acts and that they have the required resources available in order to comply. If you feel you require further training or resources or if you have any questions in relation to data protection issues then please contact the legal team.

Last reviewed : February 2021

Last updated : February 2021