

General Data Protection Regulation Policy

1. Introduction

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act and the General Data Protection Regulation (GDPR).

It applies to anyone who handles or has access to people's personal information, regardless of the way it is used, recorded, and stored and whether it is held in paper files or electronically.

2. Principles

2.1 Pabulum will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes for which it was collected.

2.2 Every effort will be made to ensure that the data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

2.3 All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed.

2.4 Pabulum will:

- ensure that information is not held longer than is necessary;
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system;
- only share personal information with others when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act;
- train all staff so that they are aware of their responsibilities and Pabulum's relevant policies and procedures.

3. Definition of Personal Data

Pabulum and individuals will have access to a range of personal data which may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families, or circumstances. This will include:

- **Employees:** Personal information about employees, temporary workers, including names, addresses, contact details, payment details, pension details, absence records, disciplinary details, employment history, taxation, national insurance records, appraisal records and references.
- **Customers:** Personal information for customers requiring a special diet. This includes customers with a medically prescribed diet such as a food allergy.



4. Responsibilities

This policy applies to all staff employed by Pabulum including temporary workers and casual members of staff. Employees, who do not comply with this policy may face disciplinary action.

4.1 Board of Directors

The Board of Directors has overall responsibility for ensuring that Pabulum complies with all relevant data protection obligations.

4.2 Data Protection Officer

Although the mandatory requirement for a Data Protection Officer (DPO) does not apply to Pabulum, the Company has voluntarily appointed a DPO. They report directly to a nominated member of the Board and operate independently and cannot be dismissed or penalised for performing their duties.

The DPO is also the first point of contact for individuals whose data Pabulum process, and the ICO.

The Name and contact details of the DPO are provided in Appendix One.

4.3 All Staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy;
- Informing Pabulum of any changes to their personal data, such as a change of address;
- Contacting the DPO in the following circumstances:
 - With questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
 - If they have any concerns that this policy is not being followed;
 - If they are unsure whether they have a lawful basis to use personal data in a particular way;
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
 - If there has been a data breach;
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - If they need help with any contracts or sharing personal data with third parties.

5. Collecting and Using Information

5.1 Lawfulness, Fairness and Transparency

Pabulum will only process personal data where it has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Pabulum can **fulfil a contract** with the individual and/or organisation or the individual has asked Pabulum to take specific steps before entering into a contract;
- The data needs to be processed so that Pabulum can **comply with a legal obligation**;



- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life such as catering for a customer with a Medically Prescribed Diet;
- The data needs to be processed to perform a task **in the public interest**, or an official function;
- The data needs to be processed for the **legitimate interests** of Pabulum or a third party (provided the individual's rights and freedoms are not overridden);
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, Pabulum will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act.

5.2 Limitation, Minimisation and Accuracy

Pabulum will only collect personal data for specified explicit and legitimate reasons. These reasons will be explained to the individuals when their data is first collected.

If Pabulum wants to use personal data for reasons other than those given when the information was first obtained, Pabulum will inform the individuals concerned before it does so and seek consent where necessary. Staff must only process personal data where it is necessary to do their jobs.

5.3 Information to Employees – the “Privacy Notice”

Pabulum will inform employees of the data we collect, process, and hold on *employees themselves*, the purposes for which the data is held and third parties to whom it may be passed. This privacy notice will be passed to employees through the induction process.

6. Secure Storage and Access to Information

6.1 Pabulum will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left in unsecured areas of Pabulum's workplaces, displayed at notice/display boards, or left anywhere else where there is general access;
- Where personal information needs to be taken off-site it must be held in lockable storage, or stored on an encrypted and password protected memory stick, or device;
- All users will use strong passwords following Pabulum's Password Construction Guidelines (available on Pabunet). Passwords will be changed regularly. User passwords must never be shared;
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto-lock if not used after 20 minutes;
- Personal data can only be stored on Pabulum owned equipment (this includes computers and portable storage media). Private equipment (i.e., owned by the users) must not be used for the storage of personal data.



- 6.2** Pabulum will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- 6.3** When personal data is stored on any laptop, another portable computer system, USB stick or any other removable media:
- the data must be encrypted, and password protected;
 - the device must be password protected;
 - where possible, the device must offer approved virus and malware checking software; and
 - the data must be securely deleted from the device, in line with Pabulum’s Retention Policy once it has been transferred or its use is complete.
- 6.4** Pabulum has clear policy and procedures for the automatic backing up, accessing and restoring of all data held on Pabulum’s systems, including off-site backups.
- 6.5** Pabulum has clear policy and procedures for the use of “Cloud-Based Storage Systems” and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. Pabulum will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

6.6 Access out of the Workplace

Pabulum recognises that personal data may be accessed by employees and other users out of the workplace. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from Pabulum workplaces or Client premises without permission and unless the media is encrypted/password protected and is transported securely for storage in a secure location;
- Users must take particular care that computers or removable devices which contain personal data are not accessed by other users (e.g., family members) when out of the workplace;
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system e.g., VPN;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;
- No data should be taken or transferred to another country, particularly outside Europe.



7. Sharing Data

7.1 Pabulum will not normally share personal data with anyone else, but may do so where:

- Suppliers or contractors need data to enable Pabulum to provide services to staff, *customers and clients* – for example, IT companies. When doing this, Pabulum will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
 - Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared;
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Pabulum.

7.2 Pabulum will also share personal data with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations.

7.3 Pabulum may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects employees.

7.4 Pabulum will not intentionally transfer personal data to a country or territory outside the European Economic Area.

8 Subject Access Requests (SAR) and Other Rights of Individuals

8.1 Subject Access Requests

Pabulum recognises that under the GDPR, data subjects have rights in connection with their personal data, the main one being the right of access. The Procedures are set out in Appendix 3 to deal with Subject Access Requests i.e., a written request to see all or a part of the personal data held by the data controller in connection with the data subject.

8.2 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information about how the information will be used and processed at the time it is collected, individuals also have the right to:

- Withdraw their consent to processing at any time;
- Request Pabulum to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;



- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Disposal of Information

9.1 Personal data that is no longer required will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

9.2 For example, we will shred paper documents and overwrite or delete electronic files. We may also use a third party to safely dispose of records on Pabulum's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

10. Personal Data Breaches

10.1 Pabulum will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 2.

10.2 When appropriate, we will report the data breach to the ICO within 72 hours.

11. Training

11.1 All staff will receive data instruction in this policy and will be made aware of their responsibilities, as described in this policy, as part of their induction.

11.2 Data protection will also form part of continuing education with all staff taking part in further training to maintain awareness of responsibilities, particularly where changes to legislation, guidance or Pabulum processes make this necessary.

12. Monitoring

12.1 Monitoring to assess compliance with this procedure will be carried out at a frequency specified by the DPO.

12.2 This policy will be reviewed and updated if necessary and at least annually.

Nelson Williams
Managing Director
July 2021



Appendix One

Name and contact details of the Data Protection Officer (DPO)

Name	Jason Hedge
Address	Linea House, Harvest Crescent, Fleet, Hampshire
	GU51 2UZ
Email	jasonhedge@pabulum-catering.co.uk
Phone	01252 819991



Appendix Two

Personal Data Breach Procedure

- 1) On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- 2) The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost;
 - Stolen;
 - Destroyed;
 - Altered;
 - Disclosed or made available where it should not have been;
 - Made available to unauthorised people.
- 3) The DPO will alert the Directors and the appropriate Data Controller.
- 4) The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- 5) The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- 6) The DPO will undertake a risk assessment to establish whether the breach must be reported to the ICO consulting the Data Controller as appropriate. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:
 - Loss of control over their data;
 - Discrimination;
 - Identify theft or fraud;
 - Financial loss;
 - Damage to reputation;
 - Loss of confidentiality;
 - Any other significant economic or social disadvantage to the individual(s) concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- 7) The DPO will document the decision (either way) in case it is challenged later by the ICO, or an individual affected by the breach.
- 8) Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned;
 - The categories and the approximate number of personal data records concerned.
 - The name and contact details of the DPO;



- A description of the likely consequences of the personal data breach;
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- 9) If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- 10) The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
- The name and contact details of the DPO;
 - A description of the likely consequences of the personal data breach;
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- 11) The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.
- 12) The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- Facts and cause;
 - Effects;
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- 13) The DPO and nominated Director will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

- 14) Pabulum will act to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The actions taken will be recorded and their effectiveness subsequently reviewed to establish whether further improvements can be made to systems and procedures.

