Data retention policy

Table of Contents

1. Recognition and definition

REGENT GAS recognizes terms such as

- “staff”, “workers”, “employees”, “colleagues” include both permanent, temporary and contractor workers
- “we”, “our”, “us” include the company, REGENT GAS
- “company” is referring to REGENT GAS

2. Definition

Data Controller:
It refers to any ‘authorised’ persons or organisation that may access and control the processing and organisation of a particular individual’s personal data.

Data Subject:
They are any living and identifiable persons whose personal data is held by an organisation.

Personal Data:
It is all data concerning a living and identifiable individual who can be identified from the information held by a Data Controller.

Processing:
It is any action that involves the deletion, disclosure, organisation, or obtaining, of the personal data.

Sensitive (non-Standard) Data:
This is Personal data that differs from standard data (name and address etc) and contains private and often highly confidential information regarding the data subject.

Third Party:
They are any persons, or organisation, other that the data subject or Data Controller.

3. Applicability

For the purposes of this Policy, the terms ‘document’ and ‘records’ include information in

- Hard Copy
- Soft copy
- Electronic form.
- Original documents
- Reproductions

4. Scope

In certain circumstances it will be necessary to retain specific documents in order to fulfill statutory or regulatory requirements and also to meet operational needs.

This policy sets

- The required retention periods for specified categories of personal data
- The standards to be applied when destroying certain information within REGENT GAS
- The disposal of records and the retention and disposal of electronic documents

This Policy applies to all REGENT GAS staff, agents, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and / or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

5. Purpose

The purpose of this Policy is to ensure that

- Necessary records and documents of REGENT GAS are adequately protected and maintained
- Records that are no longer needed by REGENT GAS or are of no value are discarded at the proper time

This Policy is also for the purpose of aiding employees of REGENT GAS in understanding their obligations in retaining documents.

6. Format of documents

Information is one of the Council's corporate assets; in the course of carrying out its' various functions.

These documents and records are in several different formats, examples of which include, (but are not limited to)

- Communications such as letters, emails and attendance notes
- Financial information including invoices, statements and reports
- Legal documents such as contracts and deeds
- Plans, drawings, photographs and tape recordings.
- Video and audio
- Data generated by physical access control systems

7. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679
- Data Protection Act 1998
- Personal Data Protection Policy

8. Requirement

To comply with the principles of the legislation records containing personal data must be:

- Disposed of appropriately to ensure that copyrights are not breached and to prevent them falling into the hands of unauthorised personnel.
- Retained for only as long as necessary.
- Retrievable and easily traced.
- Stored appropriately having regard to the sensitivity and confidentiality of the material recorded.

9. Storage

All data and records are stored securely to avoid misuse or loss. All data records are stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record. The degree of security required for file storage reflects the sensitivity and confidential nature of the material recorded. Any data file or record which contains personal data of any form is considered confidential in nature. Examples of appropriate storage include password protecting electronic documents and locking paper documents in a secure cupboard or drawer.

10. Suspension of Record Disposal

Sometimes information needs to be preserved beyond any limits set out in the Policy. The Policy shall be suspended relating to a specific customer or document and the information retained beyond the period specified in the REGENT GAS Data Retention Schedule in the following circumstances, (but are not limited to)

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual
- Information is relevant to a company in liquidation or receivership, where a debt is due to REGENT GAS
- In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm REGENT GAS or the other side's case or liability or amount involved
- If there is any doubt over whether legal proceedings, an investigation or a crime could occur, or what information is relevant or material in these circumstances
- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law

The Appointed Compliance Officer shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

11. Security of personal information

REGENT GAS will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.
REGENT GAS will store all personal information on our secure (password- and firewall-protected) servers.
All electronic financial transactions entered into through our website will be protected by encryption technology.
All electronic financial transactions entered into through our website that are handled by third party sources will be protected by the security measures put in place by the bank or organisation in question

12. Customers with an account

The Client should acknowledge that the transmission of information over the internet is inherently insecure and that REGENT GAS cannot guarantee the security of data sent over the internet.
The Client will be responsible for keeping their Username and Password used for accessing the REGENT GAS website confidential; REGENT GAS will not ask for a password other than when needed to log in to our website.

13. Retention General Principle

For any category of documents not specifically defined elsewhere in this Policy and unless otherwise mandated differently by the applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

14. Retention General Schedule

Attached as Appendix A, there is a Record Retention Schedule that is the initial maintenance, retention and disposal schedule for physical records and electronic documents of REGENT GAS.
The Appointed Compliance Officer is in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. When data is no longer required it should be appropriately destroyed.

Any retained information can only be used for the purpose for which it is stored.
The Appointed Compliance Officer is also authorised to

- Make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with legislation
- Monitor legislation affecting record retention
- Annually review the record retention and disposal program;
- Monitor compliance with this Policy.

The period of retention only commences when the record is closed.

15. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The same rules apply for the paper documents.

16. Destruction of Data

The Company and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant.

17. Disposal

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their

level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. Any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding.

The company shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out by an employee or external service provider.
The applicable statutory requirements for the destruction of information, especially requirements under applicable data protection laws, shall be fully observed.

18. Disposal method

- Non-Confidential records: place in the waste paper bin for disposal
- Confidential records*: shred documents
- Deletion of Computer Records.
- Transmission of records to an external body such as County Records Office.

* It is essential that any documents which are to be thrown away, and may contain confidential or personal data must be disposed of in this way, in order to avoid breaches of confidence.

19. Documents level of sensitivity

Documents that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data; are proprietary documents The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Documents that do not contain any confidential information or personal data and are published Company documents. These should be disposed of through a recycling bin and include, among other things, advertisements, catalogs, flyers, and newsletters.

20. Data security

Regent Gas will need to ensure that all data (hard copy or electronic) is kept securely and access is only available to authorised personnel.

All staff is responsible for ensuring that

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerised be password protected; or when kept or in transit on portable media the files must be password protected.

21. Portable device

It is the responsibility of the staff to ensure that:

- Suitable backups of the data exist ·
- Sensitive data is appropriately encrypted ·
- Sensitive data is not copied onto portable storage devices without first consulting a compliance officer, in regard to appropriate encryption and protection measures.

Electronic devices such as laptops, mobile devices and computer media (USB devices, CD's etc) that contain sensitive data are not left unattended when offsite or when non-members of the company are in the premises.

22. Breach, Enforcement and Compliance

The company has the responsibility to ensure that each of the Company's staff complies with this Policy.
Any suspicion of a breach of this Policy must be reported immediately to the appointed Compliance Officer. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.
Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings. Such non-compliance may also lead to legal action against the parties involved in such activities.

23. How to access to your data

Any questions or concerns about the policy can be raised either by
Sending a mail to data@regentgas.co.uk with the object "Subject Access Request"
Or, sending a letter by registered mail to
Regent Gas
Subject Access Request
Regent House
Kendal Ave
London W3 0XA

24. Privacy Policy Changes

Although most changes are likely to be minor, REGENT GAS may change its Privacy Policy from time to time, and in REGENT GAS' sole discretion. We encourage visitors to frequently check this page for any changes to its Privacy Policy

25. Review date

This policy will be reviewed every year or when there are technical or legislative changes that require this policy to be reviewed.

Document name:	Data retention policy
Company:	REGENT GAS
Issue date:	23-May-18
Approved by:	Deep Valecha, Operations Director
Developed by:	Alunga Kalawe, Regulation & Compliance Manager

26. Record of changes

DATE	AUTHOR	DETAILS OF CHANGE