# DATA BREACH POLICY

## Table of Contents

## 1. AIM

Regent Gas is aware of the obligations placed by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.
One such obligation is to report a breach of personal data in certain circumstances and this policy sets out Regent Gas position on reporting data breaches.
This Data Breach Policy provides general principles and approach model to respond to, and mitigate breaches of personal data (a “personal data breach”). It also lays out the general principles and actions for successfully fulfilling the obligations surrounding the notification to Supervisory Authorities and data subjects as required by the EU GDPR.

## 2. SCOPE

The Data Breach Policy applies to all staff, suppliers, organisations, governing bodies and third parties working for or acting on behalf of Regent Gas to process personal data.
.All the above mentioned people have a role to play to ensure a safe and secure work frame. They must be aware of, and follow this Data Breach Policy in the event of a personal data breach.

## 3. DEFINITIONS

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

"Data" means personal data.

“Data Protection Legislation” means (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

“GDPR (the General Data Protection Regulation)” means the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“Process” means any operations or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

## 4. PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.
The following are examples of data breaches:

a) Access by an unauthorised third party;
b) Deliberate or accidental action (or inaction) by a data controller or data processor;
c) Sending personal data to an incorrect recipient;
d) Computing devices containing personal data being lost or stolen;
e) Alteration of personal data without permission;
f) Loss of availability of personal data.

## 5. BREACH DETECTION MEASURES

Regent Gas has implemented the following measures to assist us in detecting a personal data breach:
Here are measures organizations can take to prevent data breaches from happening.

- Employ critical controls list and best practices
- Ensure data privacy awareness from the staff
- Invest in state-of-the-art cyber security (e.g. deploying anti-virus software on servers)
- Implement measures and policies that prevent or minimize security incidents
- Appoint an Compliance Officer
- Educate personnel to identify, assess, mitigate and report security incidents or personal data breaches
- Regularly monitor for security breaches and scan the vulnerability of computer networks
- Identify data sources, inventory sensitive data, and map locations
- Keep a data breach register and analyse to spot any pattern
- Regularly review and update Data Breach Policies, and other measures applicable to the system
- Formulate a data retention and data destruction policy
- Regularly update back-up or restoration systems
- Make staff aware about the GDPR and data breaches policies and process
- Make sure any external support with data are in a safe and secured place (e.g. a locked cupboards)
- Encrypt all data to log in to the website for out of the company person ( e.g. suppliers)
- Require that third parties working for or acting on behalf of Regent Gas to process personal data, are committed to be compliant with the GDPR
- Control the usage of connectable portable devices
- Change default passwords with strong one and regularly update it
- Monitor for unusual network activity and data transmissions patterns
- Only allow known traffic and applications to access or function within Regent Gas perimeter
- Maintain redundant intrusion prevention systems (iPs) and monitor their activity
- Segment production networks with firewalls and router
- Lock down iP addresses for internal and external hosts ( spam filter)
- Secure computer equipment and facilities from physical intrusion in addition to securing networks
- Make sure the servers are in safe and exclusive space (e.g. a locked room)
- Monitor network activity on wireless networks

- Reduce any data usage on mobile devices

## 6. DATA BREACH RESPONSE PROCESS

The Data Breach Response Process is initiated when anyone who notices that a suspected/alleged or actual personal data breach occurs, the appointed Compliance Officer is notified. He/she is responsible to determine if the breach should be considered a breach affecting personal data.

The appointed Compliance Officer is responsible for documenting all decisions of the core team. These documents might be reviewed by the supervisory authorities; therefore they need to be written very precisely and thoroughly to ensure traceability and accountability.

## 7. INVESTIGATION INTO SUSPECTED BREACH

In the event that Regent Gas becomes aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the appointed Compliance Officer Alunga Kalawe who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

## 8. DATA BREACH POLICY FOR MANAGING DATA SECURITY BREACHES

In line with best practice, the following steps should be immediately followed in responding to a data security breach:

- **Internal Notification:**

  Individual who has identified the breach has occurred must notify the appointed compliance officer. A record of the breach should be created using the following templates:

  a. Data Breach Incident Form
  b. Data Breach Log

- **Containment:**

Appointed Compliance Officer to identify any steps that can be taken to contain the data breach and liaise with the appropriate parties to action these.

- **Recovery:**

Appointed Compliance Officer to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause.

- **Assess the risks:**

Appointed Compliance Officer to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form

a. What type of data is involved?
b. How sensitive is it?
c. If data has been lost/stolen, are there any protections in place such as encryption?
d. What has happened to the data?
e. What could the data tell a third party about the individual?
f. How many individuals' data have been affected by the breach?
g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

## 9. RISK ASSESSMENT

The Appointed Compliance Officer will confirm receipt of this information by email.
Each Personal Data Incident must have a risk assessment performed to determine the extent and risk to the Personal Data. The risk assessment is based on facts and determines whether the Personal Data was used or disclosed in a way not permitted under GDPR policies. The risk assessment includes an evaluation of whether the incident compromises an individual's personal Data.
For the risk assessment the following steps will be carried out:

- **Data list:**

A detailed list and description of the data involved in the Personal Data Incident needs to be prepared. The list must include all the Personal Data which is potentially at risk as a result of the incident.

- **Security controls applied to the data:**

Any security controls applied to the data may limit unauthorised exposure. This may include encryption, pseudonymisation, access controls or any other controls. The security controls applied to the data should be documented.

- **Determination of risk to the individual:**

The level of risk to the individual will determine whether the Personal Data Incident is to be notified to the Supervisory Authority and/or the affected Data Subject. Determining the risk requires an evaluation of:

**(i)** The facts surrounding the Personal Data Incident;
**(ii)** An examination of the type of Personal Data;
**(iii)** The potential harm to the individual; and
**(iv)** Security controls applied.

The following factors (along with any other relevant considerations) will be considered to determine if Personal Data has been compromised:

- (a) The nature of the Personal Data Incident including where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of data records concerned;
- (b) The nature and extent of the Personal Data involved, including where Personal Data was pseudonymised data, types of identifiers and the likelihood of re- identification;
- (c) The identity of the unauthorised person who triggered the Personal Data Incident and, where applicable, or to whom it was disclosed;
- (d) Whether the Personal Data was actually acquired (including whether any security controls Regent Gas were applied to prevent access);
- (e) The likely consequences of the Personal Data Incident; and
- (f) The measures that could be taken to address the Personal Data Incident, including where appropriate, to mitigate any adverse effects.

If Personal Data is pseudonymised in accordance with applicable laws or guidance, it still qualifies as Personal Data and any inadvertent or unauthorised use or disclosure of such information will be considered a Personal Data Breach.
If Personal Data is anonymised in accordance with applicable laws and guidance, it is not Personal Data and any inadvertent or unauthorised use or disclosure of such information will not be considered a Personal Data Breach. Consult the Appointed Compliance Officer first to confirm if the data is truly anonymised.
It is important that systems and/or operations are restored as soon as possible, ensuring that this can be done without creating any further security issues or putting Regent Gas at risk of additional incidents or unintentionally discarding or destroying evidence.
Before any restoration of systems and/or data, the system should be tested to ensure it is no longer vulnerable or to prevent or minimise any potential future security risks.

## 10. WHEN A BREACH WILL BE NOTIFIED TO THE INFORMATION COMMISSIONER

In accordance with the GDPR, Regent Gas will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.
Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If Regent Gas is unable to report in full within this timescale, Regent Gas will make an initial report to the Information Commissioner, and then provide a full report in more than one installment if so required.
The following information will be provided when a breach is notified:

a) A description of the nature of the personal data breach including, where possible:
   i) The categories and approximate number of individuals concerned
   ii) The categories and approximate number of personal data records concerned
b) The name and contact details of the appointed Compliance Officer where more information can be obtained
c) A description of the likely consequences of the personal data breach

d) A description of the measures taken (or proposed to be taken) to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

## 11. PERSONAL DATA BREACH NOTIFICATION: DATA PROCESSOR TO CONTROLLER

When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, the appointed Compliance Officer of the Company acting as a data processor must report any personal data breach to the respective data controller/controllers without undue delay.

The Data appointed Compliance Officer will send Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the appointed compliance officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

## 12. WHEN A BREACH WILL BE NOTIFIED TO THE DATA SUBCJECT

In accordance with the GDPR, Regent Gas will undertake to notify the data subject whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may depend on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) A description of the nature of the breach
b) The name and contact details of the appointed Compliance Officer where more information can be obtained
c) A description of the likely consequences of the personal data breach and
d) A description of the measures taken (or proposed to be taken) to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

## 13. RECORD OF BREACHES

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

| | |
|---|---|
| **Document name:** | Data Breach Notification Policy |
| **Company:** | Regent Gas |
| **Issue date:** | 24-May-18 |
| **Approved by:** | Deep Valecha, Operations Director |
| **Developed by:** | Peninsula Business Services Limited<br>Regent Gas |