[Your Company Name]

Data Breach Policy & Procedures

DOCUMENT AUTHOR:	[Insert Author]
DOCUMENT OWNER:	[Insert Owner]
STATUS:	[Draft/Approved]
DATE CREATED:	[Insert Date]
VERSION:	[Insert Version]
LAST UPDATED:	[Insert Date]
SECURITY CLASSIFICATION:	[High/Medium/Low]

Document Customisation

This page *(to end of the 'disclaimer')* provides template guidance and ***must be removed*** from the finished version. For information on customisation, refer to the *'Instructions'* supplied in your order.

It is important to work through the document and customise any areas to ensure that the finished template accurately reflects what your organisation does and the controls that you have in place. You should consider your regulatory and legal obligations and any standards or requirements that apply to your industry or business type when customising the content.

Template Guidance

We have provided a generic template as a starting point for you to develop your own document in this compliance area. You should review and customise the template sections thoroughly to ensure that the finished version accurately reflects your organisations' controls and responsibilities.

The ***United Kingdom General Data Protection Regulation (UK GDPR),*** tailored by the ***Data Protection Act 2018 (DPA18)*** applies in the UK. Our UK GDPR templates were originally developed using the EU GDPR and DPA18 and have been subsequently updated to comply with the UK GDPR. Please refer to the BREXIT NOTE provided in the Guidance Document for further information.

Data protection compliance is not a 'one size fits all' and so it is essential that you understand your obligations under the UK GDPR (and if applicable, the EU GDPR) and that you have the correct policies and controls in place. Much of the content in our UK GDPR templates are ready to use, but each document still requires review and customisation to ensure the finished document is fit for purpose and compliant.

Referencing Other Policies

We sometimes reference other policies in a template where relevant *(i.e. refer to Anti-Bribery & Corruption Policy in conjunction with AML).* Referenced documents are **only** included in your pack if you have ordered them separately or you have purchased a Toolkit or Bundle that includes them.

Licence Terms

Purchased documents are for use within the ordering company **only** and cannot be used, sold or transferred elsewhere without written permission from Know Your Compliance Limited. Please refer to the *'Instructions'* document for more information on our T&C's and licence options.

Disclaimer

Know Your Compliance Limited has created this template for you to use in developing and implementing your compliance program requirements. Whilst every reasonable care is taken to ensure that the content is relevant, compliant and up to date; it is **your responsibility** to ensure that the finished policy complies with any regulatory and/or legal requirements and standards.

It is important that you customise the content to suit your industry needs and business type. Know Your Compliance Limited makes no claims or guarantees about the compliance or adequacy of the content in this template and accepts no responsibility or liability for any loss, damage or expense incurred as a result of reliance on the content contained herein. If you are unsure of your regulatory or legal obligations, you should obtain legal or professional advice before publishing, using or relying upon your finished policy.

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Table of Contents

1 Policy Statement 5
2 Purpose 5
3 Scope 5
4 Data Security & Breach Requirements 5
4.1 Objectives 6
5 Data Breach Procedures & Guidelines 7
5.1 Breach Monitoring & Reporting 7
5.2 Breach Incident Procedures 7
5.2.1 Identification of an Incident 7
5.2.2 Breach Recording 8
5.3 Breach Risk Assessment 8
5.3.1 Human Error 8
5.3.2 System Error 8
5.3.3 Assessment of Risk and Investigation 9
6 Breach Notifications 9
6.1 The Commissioner Notification 9
6.2 Data Subject Notification 10
7 Record Keeping 11
8 Responsibilities 11

1 POLICY STATEMENT

[Your Company Name] *(hereinafter referred to as the **"Company"**)* are committed to our obligations under the regulatory system and in accordance with the ***United Kingdom General Data Protection Regulation,*** tailored by the amended ***Data Protection Act 2018*** *(hereinafter referred to as the UK GDPR),* and maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the UK GDPR and relevant data protection laws.

2 PURPOSE

The purpose of this policy is to provide the Company's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees, ensuring that they are aware of the protocols and reporting lines for personal information data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

3 SCOPE

This policy applies to all staff within the Company (meaning permanent, fixed term, and temporary staff, any third party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 DATA SECURITY & BREACH REQUIREMENTS

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy be Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the Company. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures and Information Security Policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess

the scope and impact of any potential data breach, both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including but not limited to:-

- Pseudonymisation and encryption of personal data
- Restricted access and biometric measures
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations
- Frequent and ongoing data protection training programs for all employees
- Staff assessments and regular knowledge testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information

- Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; it is rechecked and authorised by the **[Data Protection Officer/nominated person]**

4.1 OBJECTIVES

- To adhere to the UK GDPR and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regard to personal information
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks

- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees, including their information and identity
- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues

- To ensure that the Commissioner is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of the Company having become aware of the breach

5 DATA BREACH PROCEDURES & GUIDELINES

The Company has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

5.1 BREACH MONITORING & REPORTING

The Company has appointed a **[Data Protection Officer/Compliance Officer]** who is responsible for the review and investigation of any data breach involving personal information, regardless of the level of severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and the Company retains a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revisions to any such process are recorded in our Change Management and Document Control records.

5.2 BREACH INCIDENT PROCEDURES

5.2.1 IDENTIFICATION OF AN INCIDENT

[illegible]

[illegible]

[illegible]

Page removed from sample document

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

5.3.3 ASSESSMENT OF RISK AND INVESTIGATION

The **[DPO/Compliance Officer]** should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

6 BREACH NOTIFICATIONS

The Company recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

6.1 THE COMMISSIONER NOTIFICATION

The Commissioner is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Page removed from sample document

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

7 RECORD KEEPING

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the [Data Protection Officer/Compliance Officer] and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

8 RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The [Data Protection Officer/Compliance Officer] (if applicable) is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.