



## DATA BREACH POLICY & PROCEDURE

Service With Care

## Issues And Updates Document Owner – Compliance Centre

Pages	Issue Number	Date
Review	2	Apr 24

## Background

The General Data Protection Regulation (current legislation) & Data protection Act 2018 is based around six principles of handling of personal data. We must comply with all six principles as a business; otherwise we will be in breach of the data protection legislation. We understand that the principles give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

## Aim

The current legislation requires that we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This policy sets out how we deal with a data breach.

## What is a personal data breach?

- The Information Commissioner's Office states that a personal data breach can be broadly defined as an incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

## Action to be taken in the event of a data breach

### 1. Containment and recovery

The immediate priorities are to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope.

In the event of a security incident or breach, staff must immediately inform the Data Protection Officer (via generic email [dataprotectionofficer@kingdom.co.uk](mailto:dataprotectionofficer@kingdom.co.uk) ).

The Data Protection Officer will take the lead on investigating the breach. In the event where the DPO is absent for whatever reason, the Deputy will take the lead on investigating a breach (via generic email [dataprotectionofficer@kingdom.co.uk](mailto:dataprotectionofficer@kingdom.co.uk) ).

Steps to take where personal data has been sent to someone not authorised to see it:

- Inform the recipient not to pass it on or discuss it with anyone else;
- Inform the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
- Explain to the recipient the implications if they further disclose the data; and
- Where relevant (in consultation with the Data Protection Officer), inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

## 2. Assessing the risk

Perhaps most important is an assessment of potential adverse consequences for individuals, how

serious or substantial these are and how likely they are to happen

Examples of the type of questions to consider:

What type of data is involved?	
How sensitive is it?	
If data has been lost or stolen, are there any protections in place such as encryption?	
What has happened to the data?	i.e. If stolen, could it be used for purposes which are harmful to the individuals to whom the data relate?; if it has been damaged, this poses a different type and level of risk
Estimate how many individuals' personal data are affected by the breach	
Who are the individuals whose data has been breached?	Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks

What harm can come to those individuals?	Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	
Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause	

### 3. Notifying the ICO and individuals, where relevant

#### a) Who is responsible?

In our business the Data Protection Officer is the point of contact for staff and the ICO on this policy and on all matters relating to data protection.

The Data Protection Officer is also responsible for notifying the ICO and individuals (where applicable) of relevant personal data breaches in consultation with the Data Champion of that data (individual responsible for that data set).

#### b) What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms (including reputation and financial). If it's likely that there will be a risk, then we must notify the ICO; if it's unlikely then we do not have to report it.

If we decide we do not need to report the breach, we need to be able to justify this decision, and we should document it.

#### c) When to notify the ICO and dealing with delays

Notifiable breaches must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. (This includes evenings, weekends and bank holidays.)

If we do not comply with this requirement, we must be able to give reasons for the delay. In some instances, it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Where this applies we should provide the required information in phases, as long as this is done without undue further delay.

## **d) Breach information to the ICO**

When reporting a breach, we will provide the following information:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned;
- and the categories and approximate number of personal data records concerned; · our contact person: the Data Protection Officer, via email:- [dataprotectionofficer@kingdom.co.uk](mailto:dataprotectionofficer@kingdom.co.uk) ;
- a description of the likely consequences of the personal data breach; and
- 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.

## **e) Individuals (Data Subjects)**

Where notification to individuals (Data Subjects) may also be required, the DPO will assess the severity of the potential impact on individuals as a result of the breach and the likelihood of this occurring. Where there is a high risk, those affected should be notified as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

## **f) Information to individuals**

The Data Protection Officer will consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach but will include the name and contact details of our Data Protection Officer (where relevant) or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The breach need not be reported to individuals if:

We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (eg encrypted data);

- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would involve disproportionate effort (in this case a public communication may be more appropriate).

In the case of a breach affecting individuals in different EU countries, we are aware that the ICO may not be the lead supervisory authority. Where this applies, the DPO should establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

## g) Third parties

In certain instances, the Data Protection Officer may need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial or reputational loss to individuals.

## h) Document all decisions

The Data Protection Officer must document all decisions that are take in relation to such incidents and data breaches, regardless of whether or not they need to be reported to the ICO.

### current legislation **BREACH NOTIFICATION PROCEDURE TO ICO**

	Guidance	Notes
Has there been a personal data breach?	A personal data breach occurs when there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to processed personal data	Yes – go to next question  No – breach need not be reported under regulation 33

Are there any reporting exceptions?	The breach does not need to be reported to the ICO if it is unlikely to result in a risk to the rights and freedoms of natural persons (however, it should still be reported to the DPO)	Yes – breach need not be reported No – go to next question
How long do I have to report the breach both internally and externally?	The processor must notify the controller without undue delay. The controller must notify the ICO without undue delay and, where possible, within 72 hours of becoming aware of the breach (if outside of 72 hours the report must be accompanied by reasons for the delay)	
What must the notification include?	1. The nature of the personal data breach 2. The name and contact details of the data protection officer 3. The likely consequences of the breach 4. The measures taken or proposed to be taken including proposed mitigation	
Is there any additional information to be provided?	Additional information can be provided at a later phase, but it must be provided without undue delay	
Further steps to be taken	The controller (Champion) shall document any personal data breaches comprising of the facts relating to the breach, its effects and remedial action taken. The DPO will use this report to inform the ICO of the breach	



## current legislation BREACH NOTIFICATION PROCEDURE TO DATA SUBJECT

Will the personal data breach likely result in a high risk to the rights, reputation and freedoms of natural persons?	If so, the breach must be communicated to the data subject without undue delay	<p>Yes – go to next question</p> <p>No – breach need not be reported to data subject</p>
Are there any reporting exceptions?	The breach need not be reported if: - the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (eg the data was encrypted) - the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise - it would involve disproportionate effort (in this case a public communication may be more appropriate)	<p>Yes – go to next question</p> <p>No – breach need not be reported to data subject or must be reported in a different way</p>
Who must communicate the breach?	The controller (Champion) shall communicate the personal data breach to the data subject in consultation with the DPO	
How must the breach be communicated?	Using the same content as in the notification to the supervisory authority in clear and plain language	

## 4. Evaluate our response and mitigation steps

An investigation into the cause of any breach will take place, a decision taken on remedial action and consider how we can mitigate it. As part of that process we also evaluate the effectiveness of our response to incidents or breaches.

To assist in this evaluation we consider:

What personal data is held, where and how it is stored
Risks that arise when sharing with or disclosing to others (This includes checking the method of transmission to make sure it is secure and that we only share or disclose the minimum amount of data necessary)
Weak points in our existing security measures such as the use of portable storage devices or access to public networks
Whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps
Staff awareness of security issues and look to fill any gaps through training or advice
The need for a Business Continuity Plan for dealing with serious incidents
The group of people responsible for reacting to reported breaches of security and/or data

## 5. Review

This document was created 25th March 2020 and will be reviewed annually.

Signature:



Name/Position: Chief Operating Officer

Date: 20/03/20

## APPENDIX A

### DATA SECURITY BREACH REPORTING TEMPLATE

This must be completed for EVERY data breach. Completion is required IMMEDIATELY after being notified of the breach/potential breach as the business only has a 72 hour window to inform the ICO.

This completed form should be emailed back to [dataprotectionofficer@kingdom.co.uk](mailto:dataprotectionofficer@kingdom.co.uk) asap.

PERSON REPORTING	
DATE AND TIME OF REPORT	
DATE OF BREACH	
NUMBER OF PEOPLE AFFECTED	
NATURE OF BREACH (choose most relevant) – Accidental or unlawful destruction; loss; alteration; unauthorised disclosure of, or access to processed personal data.	
DESCRIPTION OF BREACH	
HOW AND WHEN YOU BECAME AWARE OF BREACH	
DESCRIPTION OF DATA	
POSSIBLE CONSEQUENCES OF BREACH	
HAVE ALL AFFECTED INDIVIDUALS BEEN INFORMED?	
REMEDIAL ACTION TAKEN / LONG TERM ACTION RECOMMENDED (This information may not be available until after the investigation)	
OTHER PARTIES / REGULATORS INFORMED? IF SO, WHO?	