Personal Data – Breach Notification Procedure

Units 36 & 46 Coneygre Industrial Estate, Tipton, West Midlands, DY4 8XP

1. **Introduction**
   This procedure is intended for use when an incident has occurred that has resulted in a loss of personal data for which the organisation is a controller. It is a requirement of the EU General Data Protection Regulations 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and within 72 hours of the incident. When an incident affects personal data, a decision must be taken about the extent, timing and content of any communication with data subjects. The GDPR requires that communication must happen without undue delay if the breach is likely to have a high risk to the rights and freedoms of natural persons. This document should be used as guidance when responding to a breach.
2. **Personal Data Breach Notification Procedure**
   Once it has been decided that a breach of personal data has occurred there are 2 parties who may need to be informed. These are:

• The supervisory authority
• The data subject(s) affected

2.1 **Supervisory authority** The supervisory authority for Active Carriers Ltd is:
Name - Information Commissioner's Office
Address - Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone 0303 123 1113
Website https://ico.org.uk/for-organisations/report-abreach/
Email casework@ico.org.uk

2.1.1 **Deciding whether to notify the Supervisory Authority**
The GDPR requires notification if the personal data breach is likely to result in a risk to the rights and freedoms of natural persons (GDPR Article 33). The requirement is that the level of risk must be assessed by a director before deciding whether to notify. Factors to be taken into account as part of the risk assessment should include:

• Whether the personal data was encrypted
• If encrypted, the strength of the encryption used
• To what extent (if any) was the data pseudonymised (ie can a living individual be identified?)
• The data item included things such as name, address, bank details
• The volume of data involved
• The number of data subjects affected
• The nature of the breach (eg theft, accidental destruction, accidental loss)
• Any other factors that are deemed to be relevant Parties involved in this risk assessment might need to include representatives from the following areas, depending on the nature and circumstances of the breach:
• Directors
• Senior Managers
• Third party service providers
• Legal representatives

• Errors and omission insurers - The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by the Chief Executive Officer. The result of the risk assessment should include one of the following conclusions:
• The personal data breach does not require notification
• The personal data breach requires notification to the supervisory authority only
• The personal data breach requires notification to both the supervisory authority and to the affected data subjects

A Q&A is provided in Appendix 2 to help understand the requirements of breach notification.

2.1.2 **How to notify the Supervisory Authority** In the event a decision is made to notify the supervisory authority notification must be made within 72 hours from the time of becoming aware of the breach. Note – the supervisory authority will not consider non-working days/hours. If there are legitimate reasons for not making the breach notification within the time limit, these reasons must be given as part of the notification. Notification should be given via an appropriate secure method to the supervisory authority, using the form GDPR-Form-5 Personal Data Breach Notification Form as a template (see appendix 1)
More information about breach reporting can be found here: https://ico.org.uk/fororganisations/guide-to-data-protection/principle-7-security/
Written confirmation should be obtained from the supervisory authority that the personal breach notification has been received, including the date and time it was received.
Note: where necessary the notification can be "phased" in order to meet the requirement of "without undue delay".

2.2 Data Subjects
2.2.1 Deciding whether to notify data subjects The GDPR requires that a personal data breach shall be notified to the data subject when the data breach is likely to result in a high risk to the rights and freedoms of natural persons (GDPR Article 34). The risk assessment carried out in 2.1.1 will have determined whether the breach must be notified to data subjects. However, if measures have been subsequently taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required under the GDPR. When notification is required we must consider how to communicate it. The communication to the data subject should describe "in clear and plain language the nature of the personal data breach" (however see (a) below) and contain at least the information and measures referred to in points (b), (c) and (d) (See below).
(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the contact details of the data protection contact point and where more information can be obtained;
(c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
Communication is not required where:
(a) Newstead Insurance Brokers has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) Newstead Insurance Brokers has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

2.2.2 **How to notify data subjects**
As per 2.2.1 once decided if a breach requires communication to the data subject(s) affected the GDPR requires this is done without undue delay. The communication to the data subject shall describe "in clear and plain language the nature of the personal data breach. The communication must cover:
• Contact details of the contact point at our office and where more information may be obtained.
• A description of the likely consequences of the personal data breach

• A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects. In addition, it may be prudent to provide advice to the data subject regarding actions they may take to reduce the risks associated with the personal data breach, such as:
• Notify an anti-fraud agency such as CIFAS or Action Fraud
• Notify their banks to place a warning on their account not to authorise transactions such as new direct debit agreements (if financial data has been lost)
• Use the services of a credit reference agency to track where their data has been used by another individual to obtain financial services An appropriate method of communication should be used for example letter or email or both to ensure the data subject receives the communication and has the opportunity to take any action required.

Payment card breach Newstead Insurance Brokers uses third party hosted payment services which attest to PCI DSS standards of compliance. There is a risk card holder data may be at risk, although it is considered a very small risk. In the event of a breach the following steps must be taken.
• Close off payment systems
• Notify the relevant bank and third party payment service provider – do we need to appoint a forensic investigator?
• Identify and record date of intrusion
• Identify and record cause of intrusion
• Contain the breach and document how this was done
• Retrieve system and network logs
• Record which version fire wall and other cyber security measures were in place
• Identify the exposure – how many customers affected, what data was lost, what card information was lost, did it include PAN and 3 digit security codes
• Identify which cards were affected (all cards, visa, mastercard, etc etc)
• Notify the relevant law enforcement entity
• Log the law enforcement report date, case number, contact name, phone number and actions required to take
• Take advice and implement further precautions to mitigate errors, record this
• Consider the severity of the breach and whether a report must be made to the ICO – consider the fact this needs to be done within 72 hours. It may be necessary to consider performing a forensic investigation of our systems to help identify where the breach originated and understand the full scale of the breach and the risk it poses to individuals. Appendix 3 sets out information about using forensics services.

Data protection breach notification form - **ICO**

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete. If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.
Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports. In the wake of a data protection breach, swift containment and recovery of the situation is vital.
Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.
1. **Organisation details**
(a) * What is the name of your organisation – is it the data controller in respect of this breach?
(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.
(c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. Details of the data protection breach
(a) * Please describe the incident in as much detail as possible.
(b) * When did the incident happen?
(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this. (e) What measures did the organisation have in place to prevent an incident of this nature occurring?
(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. **Personal data placed at risk**
(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
(b) * How many individuals have been affected?
(c) * Are the affected individuals aware that the incident has occurred?
(d) * What are the potential consequences and adverse effects on those individuals?
(e) Have any affected individuals complained to the organisation about the incident?

4. **Containment and recovery**
(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.
(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
(c) What steps has your organisation taken to prevent a recurrence of this incident?

5. **Training and guidance**
(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.
(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. **Previous contact with the ICO**
(a) * Have you reported any previous incidents to the ICO in the last two years?
(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. **Miscellaneous**
(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
(c) Have you informed any other regulatory bodies about this incident? If so, please provide details. (d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form
Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.
What happens next?
When we receive this form, we will contact you within seven calendar days to provide:
▪ a case reference number; and
▪ information about our next steps If you need any help in completing this form, please contact our helpline on 0303 123 1113 or 01625 545745 (operates 9am to 5pm Monday to Friday)

Question & Answers

Do ALL data breaches need to be reported to the ICO?

It is only mandatory to report a personal data breach if it is likely to result in a risk to peoples rights and freedoms. (Note breaches under PECR have different notification requirements)
If the personal data breach represents a HIGH risk to peoples rights and freedoms then organisations need to report the breaches to the individuals who have been affected.
High risk might be defined as discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage. Article 34 says "The communication to the data subject … not be required 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, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption."

Do all details need to be provided as soon as possible?

We have 72 hours to notify the ICO. We don't need all the information at the outset – the ICO will not expect to receive comprehensive reports at the outset, but they will need to know the potential scope and cause of the breach, mitigation actions we plan to take and how we have planned to address the problem.

Are corporate firm's data exempt from ICO breach notification?

Myth: Companies/ organisations are not defined as 'legal' persons, therefore data which relates to the company only is not covered by GDPR.
Facts: If a business email address includes the name of individual for example, it can be considered personal data. It would identify them as an individual i.e john.smith@business.com.
Therefore any email address with an individual's name listed within it in this way must be handled under the GDPR.

Forensics services

When appointing a firm for forensics testing we should consider:
Once firm selected we need a Master Service Agreement and Statement/schedule Of Works agreed. It would be prudent to engage early with a firm, because once a breach has occurred it may be difficult to negotiate a reasonable cost, because the firm will know we urgently need assistance. Other things to consider:
Capability – how does the firm conduct its investigations?
Do they have tools that provide visibility to endpoints quickly, capture network traffic, indicators that look for the compromise – or do they image everything and conduct a manual analysis?
Do they help with containment plans and remediation recommendations?
Do they help with the remedy? Eg if large scale malware infection will they help clean the system? Do their tools actually work in our environment?
Do they understand our tools and systems? Capacity – do they have a good team?
How quickly can they operate? This will impact our system down time while the investigation takes place.
Do they offer a retainer agreement, so they are available when we need them? Experience – are they experienced in working with firms of our size?
Have they worked in our sector and dealt with similar problems?
Cost – hourly rates, budgeted hours, do they refund for unused hours/days, do we have to pay any other costs such as equipment, transport and accommodation?
Terms of agreement

- Preserve client privilege and confidentiality
- Security of information
- Limits on liability
- Indemnity if they damage our systems
- Appropriate scope of work and related costs

Name:

Job Title:

Date:

Signed: