GDPR Data Breach Policy

Policy Number	18
Version	2.0
Policy Contact	Matthew Betteridge
Date Issued	19th May 2018
Amended	19th May 2019
Next Review Date	19th May 2020
Target Audience	All OneCall24 Information users (e.g. employees, visitors, contractors, third-party organisations and data processors acting on behalf of OneCall24)
Approved by	OneCall24 Policy Team

This document defines OneCall24's Data Breach Policy ("Policy") and is to be used in conjunction with OneCall24's Data Privacy and Retention Policies to adhere to the General Data Protection Regulation (GDPR) 2018.

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. OneCall24 needs to have a robust and systematic way of responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

The Policy consists of the following sections :

1. Introduction.
2. Responsibility.
3. Our duties.
4. What can cause a personal data breach?
5. If you discover a personal data breach.
6. Managing and reporting the breach.
7. Monitoring and review.
8. Staff awareness and training.
9. Reporting concerns.
10. Consequences of non-compliance.

1 Introduction

1.1 This Data Breach Policy:

1.1.1 places obligations on staff to report actual or suspected personal data breaches; and

1.1.2 sets out our procedure for managing and recording actual or suspected breaches.

1.2 This plan applies to all staff in the UK and to all personal data and special category personal data held by One Call 24 Limited ("OneCall24"). This plan supplements our other policies relating to data protection privacy, retention and subject access requests.

1.3 The table below explains some key terminology used in this plan:

Term	**Meaning**
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed—e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of personal data.
Personal data	Information relating to an individual who can be identified (directly or indirectly) from that information.
Data subject	The individual to whom the personal data relates.
Special category personal data (sometimes known as sensitive personal data)	Personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Policy Lead	The person we appoint from time to time to lead all aspects of the development and implementation of our data protection and data privacy strategy and compliance with the GDPR and other applicable laws.
Data breach team	The team responsible for investigating personal data breaches.
Information Commissioner's Office (ICO)	The UK's independent data protection and information regulator.

2 Responsibility

OneCall's Policy Lead Susanna Caddeo has overall responsibility for this Policy. They are responsible for ensuring it is adhered to by all staff.

3 Our duties

3.1 OneCall24 processes personal data relating to individuals including staff, clients and third parties. As custodians of data, we have a responsibility under the EU General Data Protection Regulation (GDPR) to protect the security of the personal data we hold.

3.2 We must keep personal data secure against loss or misuse. All staff are required to comply with our security guidelines and policies (in particular our GDPR Data Privacy and Data Retention Policies).

4 What can cause a personal data breach?

A personal data breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored, e.g. loss of a laptop or a paper file.
- Inappropriate access controls or sharing allowing unauthorised use.
- Equipment failure, fire or flood.
- Human error, e.g. sending an email or SMS to the wrong recipient.
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing, malware and other 'blagging' attacks where information is obtained by deceiving whoever holds it.
- Information obtained by deception.
- Non-secure disposal of data,
- Unescorted visitors accessing data.

5 If you discover a personal data breach

5.1 If you know or suspect a personal data breach has occurred or may occur, you should:

5.1.1 complete a Data Breach Incident Report form. The form asks for your name, but you do not have to give it if you would prefer to report the failure anonymously;

5.1.2 email the completed form to the Head of Compliance at GDPR@onecall24.co.uk—if you wish to make an anonymous report, you can submit the form by a non-electronic method, e.g. internal post to the Head of Compliance;

5.1.3 telephone the Head of Compliance to let them know a form has been (or is being) completed on 0333 221122.

5.2 Where appropriate, you should liaise with your line manager about completion of the Data Breach Incident Report form. However, this may not be appropriate or possible, e.g. if your line manager is aware of the breach and has instructed you not to report it, or if they are simply not available. In these circumstances, you should submit the report directly to the Head of Compliance without consulting your line manager.

5.3 You should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators. The Head of Compliance will acknowledge receipt of the data breach report form (if the person making the report has given their name) and take appropriate steps to deal with the report in collaboration with the data breach team.

6 Managing and recording the breach

6.1 On being notified of a suspected personal data breach, the Head of Compliance will establish a data breach team. The data breach team will be led by the Head of Compliance.

6.2 The data breach team will take immediate steps to establish whether a personal data breach has, in fact, occurred. If so, the data breach team will take appropriate action to:

- contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;
- assess and record the breach in OneCall24's data breach register;
- notify appropriate parties of the breach;
- take steps to prevent future breaches.

These are explained in paragraphs 6.3 to 6.6.

6.3 Containment and recovery

The data breach team will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

The data breach team will identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

Depending on the nature of the breach, the data breach team will notify our insurers as the insurers can provide access to data breach management experts.

6.4 Assess and record the breach

Having dealt with containment and recovery (see paragraph 6.3), the data breach team will assess the risks associated with the breach, including:

- what type of data is involved?
- how sensitive is the data?
- who is affected by the breach, ie the categories and approximate number of data subjects involved?
- the likely consequences of the breach on affected data subjects, e.g. what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?
- where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?
- what has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?
- what could the data tell a third party about the data subject, e.g. could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?
- what are the likely consequences of the personal data breach on OneCall24, e.g. loss of reputation, loss of business, liability for fines?
- are there wider consequences to consider, e.g. loss of public confidence in an important service we provide?

Details of the breach will be recorded in OneCall24's data breach register by the data breach team.

6.5 Notifying appropriate parties of the breach

The data breach team will consider whether to notify:

- the ICO
- affected data subjects
- the police
- any other parties, e.g. insurers or commercial partners

6.5.1 Notifying the ICO

The data breach team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

If the data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: • exposure to identity theft through the release of non-public identifiers, e.g. passport number • information about the private aspects of a person's life becoming known to others, e.g. financial circumstances *The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.*
The volume of personal data	There should be a presumption to report to the ICO where: • a large volume of personal data is concerned, and • there is a real risk of individuals suffering some harm It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual. The ICO provides two examples: • loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals would be reportable • loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed would not be reportable**]**
The sensitivity of data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a

	significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples: • theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable • breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss, the koss would not be reportable**)**

6.5.2 Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach team will notify the affected data subject(s) without undue delay, including:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

When determining whether and how to notify data subjects of the breach, the data breach team will

- co-operate closely with the ICO and other relevant authorities, e.g. the police; and
- take account of the factors set out in the table below:

Factor	**Impact on obligation to notify data subject**
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data	Where such measures have been implemented, it is not necessary to notify the data subject(s).

Factor	Impact on obligation to notify data subject
subjects affected by that breach is no longer likely to materialise.	
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

6.5.3 Notifying the police

The data breach team will already have considered whether to contact the police for the purpose of containment and recovery (see paragraph 6.3). Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against or by a representative of OneCall24, the data breach team will notify the police and/or relevant law enforcement authorities.

6.5.4 Notifying other parties

The data breach team will consider whether there are any legal or contractual requirements to notify any other parties, e.g. such are any regulatory bodies or our insurers.

6.6 Preventing future breaches

Once the personal data breach has been dealt with, in accordance with this plan, the data breach team will:

- establish what security measures were in place when the breach occurred
- assess whether technical or organisational measures can be implemented to prevent the breach happening again
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- consider whether it is necessary to update our privacy risk assessment
- update OneCall24's privacy risk register
- debrief data breach team members following the investigation

7 Monitoring and review

7.1 We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least [every two years].

7.2 Our monitoring and review exercises will include looking at how our policies and procedures are working in practice to reduce the risks posed to our company.

8 Staff awareness and training

8.1 Key to the success of our systems is staff awareness and understanding.

8.2 We provide regular training to staff:

- at induction
- when there is any change to the law, regulation or our policy
- when significant new threats are identified
- in the event of an incident affecting our company or a competitor

9 Reporting concerns

Prevention is always better than cure. Data security concerns may arise at any time and we encourage you to report any concerns you have to the Head of Compliance. This helps us capture risks as they emerge, protect our company from personal data breaches, and keep our processes up-to-date and effective.

10 Consequences of non-compliance

10.1 Failure to comply with this plan and associate data protection policies puts you and OneCall24 at risk. Failure to notify the Head of Compliance of an actual or suspected personal data breach is a very serious issue.

10.2 You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.