Personal Data Breach and Incident Response Plan

Written by:
Corporate Legal Advisor

Department
Compliance

Valid from:

August 2019

Updated:

August 2021

To be reviewed by:

August 2023

This document is unsupported when printed or saved locally.

Contents

1. Policy Scope

The National Farmers Union (NFU) collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

The NFU is committed to taking appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

The purpose of this policy is to contain any data breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent any further breaches from occurring.

It is the responsibility of each NFU employee, group secretary, volunteer, contractor and worker to be aware of and to comply with this policy in the event of a personal data breach. Any breach of data protection legislation may result in the NFU's disciplinary procedures being instigated.

2. Defining a Personal Data Breach

A personal data breach is defined under Article 4 (12) of the General Data Protection Regulations (GDPR) as 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”.

A breach is therefore a type of security incident, the three different types of breach and some (non-exhaustive) examples of how these may occur are set out below:

1. **Confidentiality breach** – an accidental or unauthorised disclosure of, or access to, personal data. For example, personal data being disclosed to an unauthorised person, e.g. an email containing personal data from a member’s record being sent to the wrong person, members personal information being posted to the wrong address, or staff leaving documents containing a members personal data in a public space (such as an NFU show event).

2. **Availability breach** – an accidental or unauthorised temporary or permanent loss of access to, or destruction of, personal data. For example, where member’s data is unavailable for a certain period of time due to a misplaced decryption key for securely encrypted data or due to an accidental deletion of data by a member of staff. This type of breach can also include software or hardware failures, theft of equipment on which data is stored and also the sort of problems that might arise after a cyber attack that result in prevented access to and/or destroyed records.

3. **Integrity breach** – an accidental or unauthorised alteration of personal data. For example, during a data tampering attack where the personal data is still present but has been modified, manipulated or changed in some way.

3. Reporting an Incident

The individual, who has identified the breach has occurred, must immediately contact The Head of Compliance or alternatively notify a member of the NFU Compliance Team by emailing complianceteam@nfu.org.uk.

Full and accurate details of the incident should be recorded and maintained using the Data Breach Report Form (see Appendix 1).

4. Containment and Recovery

The Compliance Team will immediately work with the individual and any relevant department (such as IS) to firstly determine if the breach is still occurring. If so, the appropriate steps will be taken to immediately minimise the effect and contain the breach.

The Compliance Team will undertake an initial assessment to establish the severity of the breach and (depending on the nature of the breach) form the Incident Response Team (see Appendix 2) and determine who will take the lead investigating the breach. The lead investigator will identify any further steps to recover any losses and to limit or mitigate any potential damage the breach may cause. The Compliance Team will determine the suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation and Risk Assessment

Within 24 hours of the breach being discovered or reported, the Compliance Team will investigate the data breach and assess the risks associated with it. For example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will need to take into account the following: the type of data involved; its sensitivity; the protections are in place (e.g. encryptions); what has happened to the data (e.g. has it been lost or stolen; whether the data could be put to any illegal or inappropriate use; data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s); whether there are wider consequences to the breach.

The Compliance Team will record the risks associated with the breach using the Data Breach Report Form (Appendix 1).

6. Notification to the Information Commissioners Office (ICO)

Not all personal data breaches have to be notified to the ICO. Following the investigation and risk assessment, the Compliance Team must notify the ICO if the breach is likely to result in 'a risk to the rights and freedoms of data subjects'. Every incident will be assessed on a case by case basis, however, a breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- loss of control over their data or limitation of their rights
- discrimination, identity theft or fraud
- damage to reputation or financial loss or loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Compliance Team must notify the ICO without undue delay and, no later than 72 hours after becoming aware of the breach, information can be provided in phases but any late notification must explain the reasons for delay.

ICO Notification must include the following:

- A description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- A description of the likely consequences of the breach

- A description of the measures taken, or to be taken, by the NFU to address the breach and mitigate its possible adverse effects
- Full contact details of the NFU.

A record of the breach will be kept on the Compliance N:Drive of any personal data breach, regardless of whether ICO notification was required.

7. Notification to Individuals

If the personal data breach is likely to result in 'a high risk to the rights and freedoms of the individual(s)' then the individual(s) whose personal data has been affected by the incident must be notified without undue delay.

The Compliance Team will contact the individual(s) individually, by e-mail, unless that would involve a disproportionate effort, in which case the Compliance Team will work with the Communications Team to use a public communication (for example - a notification on NFUOnline and/or a press release in the Farmer and Grower magazine) and be ready to handle any incoming enquiries.

The NFU must provide the affected individuals with the following information:

- A description of the data involved, how and when the breach occurred, its nature and likely consequences.
- A description of the measures taken, or to be taken, by the NFU to address the breach and mitigate its possible adverse effects. This should include any specific and clear advice on how a data subject can themselves limit the damage, e.g. cancelling their credit cards or resetting their passwords.
- Full contact details for the NFU.

If appropriate technical and organisational protection measures have been applied to render the personal data unintelligible or subsequent measures have been taken to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise, the NFU will not need to report the breach to data subjects.

A record of the breach will be kept on the Compliance N:Drive of any personal data breach, regardless of whether any Individual(s) notification was required.

8. Notification to Third Parties

The Compliance Team must consider notifying third parties such as the police, insurers, banks, credit card companies and stakeholders such as NFU Mutual or other data controllers where we are legally obliged to or where this would be relevant to do so. A record of the breach will be kept on the Compliance N:Drive of any personal data breach, regardless of whether any notification to a third party was required.

9. Evaluation and Response

Once the initial incident is contained, the Compliance Team should carry out a full review of the causes of the breach, the effectiveness of the response and assess whether any changes need to be made to NFU policy, processes and procedures to ensure that a similar breach does not occur.

- The review may consider the following:
- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie including identifying potential weak points within existing security measures
- Whether methods of transmission are secure
- Sharing minimum amount of data necessary
- Staff Awareness Training

Appendix 1 - DATA BREACH REPORT FORM

Please act immediately to report any data breach(es). If you discover a data breach, please notify the Head of Compliance or a member of the Compliance Team immediately, complete Section 1 of this form and email it to compliance@nfu.org.uk.

Section 1: Notification of Data Security Breach: (to be completed by person reporting incident)

Date incident was discovered	
Date(s), time (s) and place(s) of actual Incident	
Name and contact details of person reporting incident	
Other staff members/departments involved in the breach?	
Description of incident and details of information lost	
Number of Data Subjects affected, if known	
Has any personal data been placed at risk? If so, please provide details:	
Brief description of any action taken at the time of discovery:	
For Use by The Compliance Team *	
Received by: **On *(date)***	
Forwarded for action to: **On *(date)***	
*Please ensure you have entered breach details on the N:Drive data breach log	

Section 2: Risk Assessment of Breach Severity

To be completed by the Lead Investigator in consultation with the Compliance Team with the Head of Department affected by the breach and if appropriate IS where applicable.

Type and description of data involved Hard Copy/Electronic. **Please include details of the IT systems, equipment, devices, records involved in the security breach:**	
What is the nature of the information lost?	
How much data has been lost? **If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?**	
Is the information unique? **Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for the NFU or third parties?**	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? **Please provide details of any types of information that fall into any of the following categories:**	
HIGH RISK personal data • Special categories personal data (as defined in the Data Protection Legislation) **relating to a living, identifiable individual's** **a) racial or ethnic origin;** **b) political opinions or religious beliefs;** **c) trade union membership;** **d) genetics;** **e) biometrics (where used for ID purposes);** **f) health;** **g) sex life or sexual orientation.**	

Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action Taken

To be completed by the Compliance Team

Incident Number	
Report received by	
On *(date)*	
Action Taken	
Notification to ICO **Is the breach likely to result in a risk to people's rights and freedoms?** Yes/No **If Yes, then the ICO should be notified within 72 hours.** **Date and time ICO notified:** **Reported by:** **Method used to notify ICO:** **Further Notes**	
Notification to Data Subjects **Is the breach likely to result in a high risk to people's rights and freedoms?** Yes/No **If Yes, then the individual should be notified.** **Date individual notified:** **Notified by:** **Further Notes:**	

Notification to Third Parties/stakeholders Names, Date notified and method of notification. **Further Notes:**	

Section 4: Recommendations to be implemented:

Internal procedures to be completed/outline of the details of steps needed to prevent reoccurrence of breach: (e.g. disciplinary investigation, training, policy updates, new process to implement) to be completed	

Appendix 2: The Incident Response Team

Purpose: To assist the Compliance Team to deal effectively with a data breach.

Note: this is a suggested team of individuals likely to be required to deal with more serious and complex data breaches. The Compliance Team will determine whether an Incident Response Team is required to deal with the breach. Where necessary, the Incident Response Team should convene as soon as possible after the data breach occurs. Depending on the type of breach, the Incident Response Team may comprise of the following individuals from the various departments:

Compliance: To lead and co-ordinate the Incident Response Team and data breach response.

Information Services (IS): To provide guidance of IT Systems and security controls, to help identify what data has been compromised, to assist with implementing mitigating actions to contain and recover electronic data, equipment and devices.

HR: To provide guidance, knowledge and management of staff data to help identify what staff data has been compromised.

PR/Internal Communications: To provide Expert advice on communications regarding the data breach. For example, formulating messages to media and other external parties, dealing with press enquiries, and assisting with drafting internal messages on the breach.

Compliance Property: To provide knowledge and management of building security controls, to help identify what information has been compromised and help implement mitigating actions to contain, recover data or equipment.

Other various departments: As required.

Process Map