NFU Policy

Data Protection Policy for Officeholders

Written by:
Corporate Legal Adviser

Department
Compliance

Valid from:

May 2023

To be reviewed by:

May 2024

As an Officeholder, you are expected to read and comply this policy, which gives important information about:

- The data protection principles with which the NFU must comply;
- What is meant by personal data;
- How the NFU gathers, uses and (ultimately) deletes personal data in accordance with the data protection principles;
- Where more detailed privacy information can be found;
- The rights and obligations in relation to data protection; and
- The consequences of failure to comply with this policy.

Once you have read and understood this policy along with the other accompanying Officeholder policies in the Officeholder area of NFU Online, please sign and return the acceptance form to your [Chief Adviser, Regional Director, Board Secretary]. An electronic signature is acceptable.

The form is available in the Officeholder area of NFU Online.

Introduction

The NFU is a membership organisation which holds and processes a great deal of personal data relating to members, staff, officeholders and other individuals. The NFU's activities are governed by the following data protection legislation: the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

As an Officeholder it is important that you understand what your obligations are in relation to data protection legislation to ensure that the NFU can comply with its legal obligations.

This policy sets out how the NFU complies with its data protection obligations. Its purpose is also to ensure that Officeholders understand and comply with the rules governing the collection, use and deletion of personal data which they may have access to in the course of their Officeholder duties.

Officeholders should also refer to the NFU's Data Protection Privacy Notice along with other relevant Officeholder Guidance and Policies which contain further information regarding the protection of personal data. These documents are listed at the end of the document.

The NFU Compliance Department is responsible for data protection compliance within the NFU. If you have any questions or comments about the content of this Policy or if you need further information, please email complianceteam@nfu.org.uk.

The UK General Data Protection Regulation (GDPR)

The GDPR is designed to protect personal information which is processed by organisations like the NFU. It applies to personal data, which is data where an individual can be identified from, this includes, amongst other things, names, identification numbers and location data.

The GDPR applies to both automated personal data (such as phones and computer systems) and manual filling systems (such as paper files).

The Data Protection Principles

The GDPR defines seven Data Protection Principles which set out the main responsibilities for an organisation and which protect the rights of individuals. Officeholders should familiarize themselves with these principles as the NFU is required to comply with these principles.
A failure to comply leaves the NFU, its employees and Officeholders open to sanctions and enforcement action from the Information Commissioner's Office (ICO).

The principles can be summarised as follows:

1. Lawfulness, fairness and transparency – personal data shall be processed with a lawful basis, in line with a clear privacy notice and the data will be used in a way an individual would expect it to be used.
2. Purpose limitation – personal data shall be collected for specified, explicit and legitimate purposes and will not be processed in a way that is incompatible with those legitimate purposes;.
3. Data minimisation – personal data shall be adequate, relevant and limited to what is necessary for the purpose.
4. Accuracy – personal data must be accurate, kept up to date and, if inaccurate, erased or rectified without delay.
5. Storage limitation – personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary.
6. Integrity and confidentiality – personal data shall be processed in a manner that ensures appropriate security and protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
7. Accountability – the controller is responsible for the data it holds and shall demonstrate compliance with the principles.

Please ensure you understand how these principles relate to your activities as an Officeholder when dealing with personal data.

Lawful basis for processing personal data

In order for the NFU to process any data, the NFU has to have a lawful basis to do so.

Before processing data, the NFU will review the purposes of the particular processing activity and select the most appropriate lawful basis (or bases) for that processing. This will be done at the outset and at regular intervals thereafter.

The following are the lawful bases under GDPR which the NFU can rely on:

- Consent
- Contract
- Legal obligation
- Vital interest
- Public task
- Legitimate interest

The most common grounds of processing for the NFU are contract, legitimate interest and consent.

The NFU must document its decision as to which lawful basis applies, to help demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for processing in the NFU privacy notice.

Special category and criminal records data is more sensitive and legally will require more protection. Please contact the Compliance Department to obtain further advice if you envisage processing special category or criminal records data.

Individual rights

Individuals have certain rights in relation to their personal data and these are listed below:

1. To be informed about how, why and on what basis their data is processed by the NFU, please see the NFU's Privacy Notice.
2. To obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a data subject access request;
3. To have data corrected if it is inaccurate or incomplete;
4. To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing;
5. To restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful or where the NFU no longer needs the personal data; and
6. To restrict the processing of personal data temporarily where you do not think it is accurate (and the NFU is verifying whether it is accurate), or where you have objected to the processing.

It is important to bear in mind that individuals have rights under the GDPR including to see whatever data the NFU holds on them (Subject Access Request). Therefore, we expect that the content of any records, emails or calls to CallFirst concerning any individuals are factual and objective. Please do not make comments which may cause embarrassment or distress to the individual concerned or the NFU.

If an Officeholder is approached by an individual or a member in relation to any of these rights the Officeholder should immediately contact a member of the Compliance Department by emailing complianceteam@nfu.org.uk so that the request can be dealt with in line with the statutory deadlines.

Your Obligations

When handling personal data, you must:

1. Comply with the Data Protection Principles outlined above and in this document;
2. Only access the personal data that you have authority to access, and only for authorised purposes;
3. Only allow other NFU Officeholders and staff to access personal data if they have appropriate authorization. If you are uncertain, please contact your Regional Office.
4. Only allow individuals who are not NFU Officeholders or staff to access personal data if you have specific authority to do so from the Compliance Department.
5. Keep personal data secure by complying with the NFU's Information Security Policy and other supporting Officeholder documents on NFU Online.
6. Not remove personal data, or devices containing personal data (or which can be used to access it), from NFU premises unless appropriate security measures are in place (such as encryption, password protection or pseudonymisation) to secure the data and the device.
7. It is vital that any data which is shared with you as part of your role as an NFU Officeholder is treated as confidential and is only used for the purposes for which it has been disclosed. If you wish to have access to member data, your Regional Director will assist with this in order to determine whether this information can be shared. Where any data is shared with an Officeholder it is vital that it is only used for an agreed, specified purpose, that it is destroyed or returned as soon as that purpose has been fulfilled.
8. Any documentation shared with Officeholders for the purposes of NFU business must, where possible, be anonymized and where this is not possible Pseudonymized.
9. Upon ceasing to be an Officeholder for the NFU, all NFU information, documents and data, both electronic and hard copy must be promptly destroyed, deleted or returned to the NFU for secure destruction.
10. Any Data Breaches must be reported as soon as possible to the Compliance Team. Complianceteam@nfu.org.uk in line with the Data Breach Policy.
11. A Confidentiality Agreement is available in the Governance Handbook of the website. Please sign this agreement and return it to your Regional Director or Board Secretary.

Data breaches

- A data breach may take many different forms, for example:
- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where data is obtained by deceiving the organisation which holds it.
- In some cases, the NFU will need to report a data breach to the information commissioner's office within 72 hours. Please see the data breach policy for more information.

Consequences of failing to comply

The NFU takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal data is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and the NFU; and may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an Officeholder's failure to comply with any requirement may result in disciplinary action under the Code of Conduct.

Definitions:

Data Protection Legislation	The UK General Data Protection Regulation and The Data Protection Act 2018.
Data Subject	The individual to whom the personal data relates
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.
Personal Data	Sometimes known as personal information. Data relating to an individual who can be identified (directly or indirectly) from that data.
Processing	Obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying data, or using or doing anything with personal data.
Pseudonymised	The process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.
Special Category Data	Sometimes known as 'special categories of personal data', 'sensitive personal data' or 'sensitive personal information'. Personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.