NCFRS Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy regarding the data protection obligations of the National Co-operative Farm Relief Services (NCFRS) organization including: FRS Recruitment, FRS Training, FRS Fencing, Farm Relief Services and Herdwatch.

NCFRS is a data controller with reference to the personal data which it manages, processes and stores.

Employees/clients of NCFRS should refer to the guidance provided by the Office of the Irish Data Protection Commissioner (www.dataprotection.ie) as well as seeking professional advice regarding best practice in this area.

Rationale

As a data controller, NCFRS and its staff (hereafter referred-to collectively as FRS or FRS Network) must comply with the data protection rules set out in the relevant Irish legislation.

This Policy applies to all personal data collected, processed and stored by FRS in the course of its activities.

To the extent that FRS's use of personal data qualifies as 'business to customer' processing, including the organisation's communications to its staff members, the organisation is mindful of its obligations under the relevant Irish legislation, namely:

- The Irish Data Protection Act (1988);
- The Irish Data Protection (Amendment) Act (2003); and
- The EU Electronic Communications Regulations (2011).
- The GDPR (General Data Protection Regulations, 2018)

Scope

The policy covers both personal and sensitive personal data held in relation to its data subjects by FRS. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by FRS. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy.

Data	This includes both automated and manual data. • Automated data means data held on computer, or stored with the intention that it is processed on computer. • Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information that relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of FRS.
Sensitive Personal Data	Sensitive personal data is personal data which relates to specific aspects of one's identity or personality, and includes information relating to ethnic or racial identity, political or ideological beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record.
Data Controller	The legal entity responsible for the acquisition, processing and use of the personal data. In the context of this policy; NCFRS is the data controller.
Data Subject	A living individual who is the subject of the personal data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes personal data on behalf of FRS on the basis of a formal, written contract, but who is not an employee of FRS.

Data Protection Officer/ Co-ordinator	A person appointed by FRS to monitor compliance with the appropriate data protection legislation, to deal with Subject Access Requests, and to respond to data protection queries from staff members and the general public.

NCFRS as a Data Controller

In the course of its daily organisational activities, FRS acquires, processes and stores personal data in relation to living individuals. To that extent, FRS is a data controller, and has obligations under the Data Protection legislation, which are reflected in this document.

In accordance with Irish Data Protection legislation, this data must be acquired and managed fairly.

FRS is committed to ensuring that all staff members have sufficient awareness of the legislation in order to be able to anticipate and identify a data protection issue, should one arise. In such circumstances, staff members must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by FRS, there is a regular and active exchange of personal data between FRS and its data subjects. In addition, FRS exchanges personal data with data processors on the data subjects' behalf. This is consistent with FRS's obligations under the terms of its contracts with its data processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer to seek clarification. (www.dpo@frsnetwork.ie)

Third-Party Processors (where applicable)

In the course of its role as data controller, FRS engages third-party service providers, or data processors, to process personal data on its behalf.

In each case, a formal, written contract will be put in place with the processor, outlining their obligations in relation to the personal data, the security measures that they must have in place to protect the data, the specific purpose or purposes for which they are engaged, and the understanding that they will only process the data in compliance with the Irish Data Protection legislation.

The contract will also include reference to the fact that the data controller is entitled, from time to time, to audit or inspect the data management activities of the data processor, and to ensure that they remain compliant with the legislation, and with the terms of the contract.

The Data Protection Rules

The following key rules are enshrined in Irish legislation and are fundamental to FRS's data protection policy.

In its capacity as data controller, FRS ensures that all data shall:

1. *Be obtained and processed fairly and lawfully*

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the data controller (FRS);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the data controller;
- Any other information that is necessary so that the processing may be fair.

FRS will meet this obligation in the following way:

- Where possible, the informed consent of the data subject will be sought before their data is processed;
- Where it is not possible to seek consent, FRS will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where FRS intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view, prior to the recording;
- Processing of the personal data will be carried out only as part of FRS's lawful activities, and it will safeguard the rights and freedoms of the data subject;

- The data subject's data will not be disclosed to a third party other than to a party contracted to FRS and operating on its behalf, or where FRS is required to do so by law.

2. Be obtained only for one or more specified, legitimate purposes

FRS will obtain data for purposes which are specific, lawful and clearly stated. A data subject will have the right to question the purpose(s) for which FRS holds their data, and it will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s)

Any use of the data by FRS will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure

FRS will employ high standards of security in order to protect the personal data under its care. FRS's Password Policy and Data Retention & Destruction Policies guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by FRS in its capacity as data controller.

Access to, and management of, staff and customer records is limited to those staff members who have appropriate authorisation and password access.

In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third party processor will notify the data controller without undue delay.

5. Be kept accurate, complete and up-to-date where necessary

FRS will:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. FRS conducts a review of sample data every six months to ensure accuracy;

- Ensure that staff contact details and details on next-of-kin are reviewed and updated every two years, or on an 'ad hoc' basis where staff members inform the office of such changes;
- Conduct regular assessments in order to validate the need to keep certain personal data.

6. *Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed*

FRS will ensure that the data it processes in relation to data subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. *Not be kept for longer than is necessary to satisfy the specified purpose(s)*

FRS has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, FRS undertakes to destroy, erase or otherwise put this data beyond use.

8. *Be managed and stored in such a manner that, in the event a data subject submits a valid Subject Access Request seeking a copy of their personal data, this data can be readily retrieved and provided to them*

FRS has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, FRS's staff engages in active and regular exchanges of information with data subjects. Where a valid, formal request is submitted by a data subject in relation to the personal data held by FRS which relates to them, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which FRS must respond to the data subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

FRS's staff will ensure that such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request.

Implementation

As a data controller, FRS ensures that any entity which processes personal data on its behalf (a data processor) does so in a manner compliant with the Data Protection legislation through a formal Data Processor Agreement.

Regular audit trail monitoring will be done by the Data Protection Officer to ensure compliance with this Agreement by any third-party entity which processes personal data on behalf of FRS.

Failure of a data processor to manage FRS's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of FRS's staff to process personal data in compliance with this policy may result in disciplinary procedings.