RCNI
Carmichael Centre
North Brunswick Street
Dublin 7

Web: www.rcni.ie
Email: admin@rcni.ie

Data Retention Standard 2018

1. Purpose of this Policy

The Data Protection Acts 1988 and 2003 (as amended) and 2018 (the DPA) and, from the 25th of May 2018, the General Data Protection Regulation (the GDPR) impose obligations on us, as a Data Controller, to process personal data in a fair manner.

Under these rules, individuals have a right to be informed about how their personal data is processed. The GDPR sets out the information that we should supply to individuals and when individuals should be informed of this information. We are obliged to provide individuals with information on our retention periods or criteria used to determine the retention periods.

The length of time for which RCNI needs to retain Personal Data is set out in the RCNI '**Personal Data Retention Schedule**'. This takes into account the legal and contractual requirements that influence the retention periods set forth in the schedule.

All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

1.1. Grounds for processing

RCNI are required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data.

The 6 legal grounds for processing personal data are as follows:

1.1. Consent;

1.2. Performance of a contract;

1.3. Legal obligation;

1.4. Vital interest;

1.5. Public interest;

1.6. Legitimate interest

Explicit consent is required where special categories, also known as sensitive personal data are being processed.

RCNI may be able to rely on more than one legal basis for collecting personal data.

If there is no justification for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future. Consent must be obtained in advance.

In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing.

1.2. **Further Processing**

Retention of personal data is lawful only when it is compatible with the purposes for which it was originally collected.

1.3. **Right of Erasure**

Individuals have the right to have their personal data erased and no longer processed in the following circumstances:

- Where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- Where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her;
- Where the processing of his or her personal data does not otherwise comply with the GDPR

2. Document Retention Procedure

2.1. As an organisation, RCNI is required to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

- Fines and penalties;
- Loss of rights;

- Obstruction of justice charges;
- Contempt of court charges;
- Serious disadvantages in litigation

2.2. RCNI retain certain records because they contain information that:

- Serves as RCNI's organisational memory;
- Have enduring organisational value, for example, they provide a record of a transaction, evidence RCNI's rights or obligations, protect our legal interests or ensure operational continuity;
- Serves to enable the functions and business of the RCNI
- Must be kept in order to satisfy legal, accounting or other regulatory requirements

2.3. RCNI aim to balance these requirements with our statutory obligation to only keep records for the period required and to comply with data minimisation principles. The retention schedule below sets out the relevant periods for the retention of RCNI's documents.

3. Types of Documents

This policy explains the differences among records, disposable information, personal data and confidential information belonging to others.

3.1. **Records**

A record is any type of information created, received or transmitted in the transaction of RCNI's business, regardless of physical format. Examples of, but not limited to, where the personal data may be located are:

- Appointment books and calendars
- Audio and video recordings
- Computer and software programs
- Contracts
- Forms
- Electronic/digital files
- E-mails and their attachments
- Handwritten notes
- Invoices
- Letters and other hard copy correspondence
- Memory in mobile phones

- Online postings, such as on Facebook, Twitter and other sites
- Servers – own or third party
- Voicemails

Therefore, any paper records and electronic files, that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix to this policy, must be retained for the amount of time indicated in the Records Retention Schedule.

A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention.

If you are unsure whether to retain a certain record, seek expert advice. .

3.2. **Disposable Information**

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated;
- Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record;
- Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of RCNI and retained primarily for reference purposes;
- Spam and junk mail

3.3. **Personal Data**

Personal Data is defined as any data which can identify an individual either on its own or when combined with other data which we possess.

3.4. **Confidential Information**

Any confidential information obtained by a member of staff/volunteer must not, so long as such information remains confidential, be disclosed to or used by RCNI.

Unsolicited confidential information submitted to RCNI should be refused, returned to the sender where possible, and deleted if received electronically.

4. The role of the Data Compliance Officer in Records Management

The Data Compliance Officer, in conjunction with the Board, is responsible for identifying the documents that RCNI must or should retain, and determining the proper period of retention. The responsibilities of the Data Compliance Officer include oversight of the following:

- Arranging for the proper storage and retrieval of records;
- Handling the destruction of records whose retention period has expired;
- Planning, developing and prescribing document disposal policies, systems, standards and procedures;
- Monitoring compliance so that employees know how to follow the document management procedures;
- Developing and implementing measures to ensure staff know what information RCNI has and where it is stored, that only authorised users have access to certain information, and that RCNI keeps only the information it needs;
- Establishing standards for filing and storage equipment and recordkeeping supplies;
- In cooperation with the Board, establish a disaster plan to ensure maximum availability of RCNI records in order to re-establish operations quickly and with minimal interruption and expense;
- Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system;
- Periodically review the records retention schedules and legislation to determine if RCNI's document management program and its Records Retention Schedule is in compliance with legislation.
- Inform staff and the Board of any laws and administrative rules relating to corporate records;
- Explain to new staff/volunteers their duties relating to the document management;
- Ensuring that the maintenance, preservation, and destruction of RCNI records is carried out in accordance with this policy and our legal requirements.
- Planning the timetable for the annual records destruction exercise and the annual records audit;
- Evaluating the overall effectiveness of the document management program;
- Reporting annually to the Board on the implementation of the document management program

5. How to Store and Destroy Records

5.1. **Storage**

RCNI records must be stored in a safe, secure and accessible manner.

Any documents and financial files that are essential to operations during an emergency must be duplicated and/or maintained off site such as in the cloud storage.

5.2. **Destruction**

RCNI is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction.

The destruction of hard copy personal data, confidential, financial and personnel-related records must be conducted by shredding.

The destruction of electronic records must be deleted and archived, download and back up versions deleted and bins emptied. ?

The destruction of records must stop immediately upon notification that a litigation hold is to begin because RCNI may be involved in a litigation or an official investigation. Destruction may begin again once the relevant litigation hold is lifted.

6. Questions About the Policy

Any questions about this policy should be referred to the Data Compliance Officer who is in charge of administering, enforcing and updating this policy.

7. Retention Schedule