

Data Retention Policy for Compliance Interventions

**This document should be read in conjunction with section 905
of the Taxes Consolidation Act 1997**

This document was created June 2017

Contents

1. Introduction	3
2. Compliance Interventions	3
3. Access to Traders Records	4
3.1 Power to Copy, Extract, Remove	4
3.2 Removal of Actual Records	4
3.3 Copies or Extracts	4
3.4 Nature of Copies/Extracts	5
3.5 Sensitivities Regarding Commercial Data	5
4. How Does Revenue Get The Data?	5
4.1 Data Exchange	5
4.2 Revenue File Transfer Service (RFTS)	6
4.3 ROS Upload	6
4.4 Encrypted USB Keys	6
5. What Happens When The Data Arrives In Revenue?	6
6. Can The Data Be Used For Any Other Purpose?	6
7. Are There Data Protection Issues?	7
8. Period of Retention	8
8.1 Period of Intervention	8
8.2 How Long Should Revenue Retain The Data?	8
8.3 Data Retention After The Intervention Has Closed	8
9. Summary	9
9.1 Actual Records	9
9.2 Copy Records	9
9.3 Further Checking	9
9.4 Compliance Intervention Workings	9
9.5 Revenue File Transfer Service	9
10. Implementation	10

1. Introduction

The purpose of all Revenue interventions is to seek assurance that a business has filed true and correct tax returns based on the information contained in the underlying records, whether computerised or not. Increasingly, audit and other compliance interventions are conducted using analysis of electronic data using IDEA or other tools. The [Code of Practice for Revenue Audit and other Compliance Interventions](#) applies to these e-Interventions in the same way as any other intervention.

There are however, specific legal requirements relating to the keeping of electronic records contained in sections 886 (Obligation to keep certain records) and 887 (Use of electronic data processing) TCA 1997 and in the related [“Information Technology & Procedural Requirements”](#) which were last updated and re-published in May 2017. Specific VAT-related rules are set out in Regulation 21 of the Value Added Tax Regulations 2010.

Section 851A (Confidentiality of taxpayer information) TCA 1997 makes it an offence for a Revenue officer to disclose taxpayer information other than in accordance with that section or by any other statutory provision.

Section 912 (Computer documents and records) TCA 1997 provides that any requirement on a person to retain and produce records and any power of inspection by an officer of the Revenue Commissioners applies also where the data is stored electronically. The taxpayer is expected to fully co-operate with the Revenue caseworker. The Revenue caseworker may require reasonable assistance in obtaining or retrieving information or data from electronic sources from the person by, or on whose behalf, the electronic data is being used, from the operator of the equipment or from the supplier of software supporting the electronic records..

All case workers must familiarise themselves with [Revenue’s Data Security Policy](#) and ensure they act in accordance with that policy before, during and after the compliance intervention.

2. Compliance Interventions

By far, most electronic data acquired will arise from e-Audit interventions. This paper will focus, primarily, on these although similar issues will arise in the case of other intervention types where electronic data is acquired. Further guidance is provided in the [Code of Practice for Revenue Audit and other Compliance Interventions](#).

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

3. Access to Traders Records

3.1 Power to Copy, Extract, Remove

Section 905 (2) (Inspection of documents and records) TCA 1997 provides, inter alia, that an authorised officer may enter any business premises and require that business records be produced to him/her, in order to:-

- examine any records or property and take copies of or extracts from any records,
- remove any records and retain them for a reasonable time for the purposes of their further examination or for the purposes of any legal proceedings instituted by an officer of the Revenue Commissioners or for the purposes of any criminal proceedings.

Section 108 (2) (d) (Inspection and removal of records) VAT Consolidation Act 2010 provides that an authorised officer may, in the case of any such books, records, accounts or other documents produced to, or found by, the authorised officer, take copies of or extracts from them and remove and retain them for such period as may be reasonable for their further examination or for the purposes of any proceedings in relation to tax.

Section 912 TCA 1997 applies the above provisions to electronic records.

The distinction between taking copies or extracts from records and the removal of actual records is an important one for the purpose of retention.

3.2 Removal of Actual Records

Removal of actual records occurs infrequently.

The retention period of these records is finite and is governed by section 905(2)(iv) (D) TCA 1997, that is, ***“for a reasonable time”***.

3.3 Copies or Extracts

All e-Interventions will involve acquisition of copies of records or extractions from records. Typically, extracts from, or copies of, records will include any one or more of the following:

- copies of “raw data” in a database, involving the underlying transactions, e.g. individual line level transactions in an EPOS system,

- reports from systems, e.g. reports of sales, purchases, payments, bank etc.,
- reports from non financial business records such as tachograph records, stock control, and manufacturing processes.

3.4 Nature of Copies/Extracts

The nature of these copies/extracts is that they are not the taxpayer's records but copies thereof. They are more akin to photocopied and printed records that might be acquired as part of a paper based compliance intervention.

3.5 Sensitivities Regarding Commercial Data

Certain taxpayers, in the process of a Revenue compliance intervention, have expressed concern in relation to commercially sensitive data which Revenue requires to copy or extract from their records. These taxpayers often have strict security policies in relation to their own operations.

To this end, Revenue has established an information security management system (ISMS) which operates all the processes required to identify the information we need to protect and how we must protect it. The ISMS is constantly reviewed to keep it up to date and is externally validated, by a certified Third Party, twice yearly. The ISMS management system conforms to ISO 27001 and ISO 22301 standards.

All Internet facing Revenue systems, including the Revenue File Transfer Service (see 4.2) are subject to 3rd party penetration testing.

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

4. How Does Revenue Get The Data?

4.1 Data Exchange

Revenue has high standards of physical and technical security to protect confidentiality of personal data. Revenue has a set of security measures in place, including the standard of data security expected of all employees. A range of measures currently in place include restricted access to data, protocols on the use of storage devices, and a high level of encryption.

The approved methods for data exchange for e-Interventions are the Revenue File Transfer Service and Revenue encrypted USB keys. Secure email using My-Enquiries and encrypted TLS Email can also be used for data exchange during a compliance intervention but these methods are limited to

small files and are more suited to email type discussion rather than data exchange.

4.2 Revenue File Transfer Service (RFTS)

The Revenue File Transfer Service (RFTS) is a service designed for caseworkers to receive files from customers. It was designed with ease of use and security in mind. All files and accompanying notes are fully encrypted in transit and at rest. All files uploaded are virus scanned. All user data is stored on a secure Revenue LAN. The RFTS is physically located in Revenue's ISO 27001:2013 accredited data centre in Dublin.

Customers can transfer files with a maximum capacity of 2GB and do not require a ROS Certificate. This is important for smaller traders where the agent rather than the customer would, generally, have a ROS certificate. The interface is modern and designed to be easy to use. The RFTS can also be used by all caseworkers, reducing the use of USB keys in the medium term while improving usability for the customer.

4.3 ROS Upload

4.4 Encrypted USB Keys

A Revenue Encrypted USB key is another method of data transfer for compliance intervention purposes. They are relatively fast compared to the other methods especially for smaller customers and can be used to transfer large files. In any event, this is the least preferred option for data exchange from Revenue's point of view and should only be used in exceptional circumstances.

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

5. What Happens When The Data Arrives In Revenue?

The current procedure is to store the original data on a secure drive (i.e. a secure Revenue server) at the earliest opportunity.

6. Can The Data Be Used For Any Other Purpose?

Section 872 (Use of information relating to other taxes and duties) TCA 1997 provides that:

“872 (1) Any information acquired, whether before or after the passing of this Act, in connection with any tax or duty under the care and management of the Revenue Commissioners may be used by them for any purpose connected with any other tax or duty under their care and management.

(2) The Revenue Commissioners or any of their officers may, for any purpose in connection with the assessment and collection of income tax, corporation tax or capital gains tax, make use of or produce in evidence any returns, correspondence, schedules, accounts, statements or other documents or information to which the Revenue Commissioners or any of their officers have or has had or may have lawful access for the purposes of the Acts relating to any tax, duty, levy or charge under the care and management of the Revenue Commissioners.”

Data acquired may therefore be used in relation to another tax or for any purpose in connection with assessment and collection of Income Tax, Corporation Tax or Capital Gains Tax or for any purpose connected with any other tax or duty under Revenue’s care and management.

7. Are There Data Protection Issues?

While the data acquired is business data, we are not restricted in its use or retention by virtue of Section 8 of the Consolidated Data Protection Acts 1988 and 2013 which exempts data:

“(b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid,

(e) required by or under any enactment or by a rule of law or order of a court.”

Neither the Taxes Acts nor the VAT Acts impose any restriction on the retention of copy records or extractions.

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

8. Period of Retention

8.1 Period of Intervention

At a minimum, the data must be kept until the compliance intervention is closed. Summaries and test files created as a result of the analysis of the data require that the underlying records remain in IDEA so that the tests can be re-run or further tests conducted. Also, it may be necessary to export subsets of the data to a spreadsheet for presentation to the taxpayer or agent.

8.2 How Long Should Revenue Retain The Data?

Current Procedure

In relation to paper based compliance interventions, any original paper documentation is returned to the taxpayer once the intervention has been finalised and all issues resolved, i.e. where there is no further business reason for retaining it. Copied documentation is either left on file or destroyed. Caseworkers delete the underlying data once the intervention is finally closed i.e. approved at the highest level required. The results or working papers are held indefinitely on the caseworker's secure drive.

8.3 Data Retention After The Intervention Has Closed

Following the closing of the intervention, the original data may be required in relation to:

- a request, by the taxpayer, to review the outcome of the intervention,
- a quality assurance review of the intervention,
- Revenue's Internal Audit, or
- a subsequent intervention in the case.

For these purposes, the caseworker will retain on the secure drive the results of the analysis, which, as stated above are the IDEA "Test Files" of the intervention.

In addition, in relation to quality control, the Original Copies, Working Copies and Underlying Data are to be retained for a period of six months following the compliance intervention outcome becoming final.

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

9. Summary

9.1 Actual Records

In relation to a person's actual records the same retention rules apply to original electronic records as apply to original paper based records. Revenue is entitled to retain actual records for a reasonable period of time for the purpose of their examination or legal proceedings. Implicit in this is that these records should be returned once a compliance intervention or legal proceedings have been completed. In practice, however, actual records (paper or electronic) are rarely uplifted.

9.2 Copy Records

The e-Intervention Original Copies, Working Copies and Underlying IDEA files should be destroyed (in the sense that the data should not be capable of being recreated by reasonable efforts) once the compliance intervention is closed and a period of six months has passed.

9.3 Further Checking

Caseworkers are reminded that the data received can only be used within the scope of section 872.

9.4 Compliance Intervention Workings

The results or IDEA "Test Files" should be held on the caseworker's secure electronic drive where they can be accessed (on a restricted basis) for the purposes of any internal or external review or to inform a subsequent intervention. These should be retained in accordance with Revenue's general policy on data retention.

9.5 Revenue File Transfer Service

The Revenue File Transfer Service is the preferred method for caseworkers to receive files from taxpayers.

The following material is either exempt from or not required to be published under the Freedom of Information Act 2014.

[...]

10. Implementation