

Scottish Data Deletion Automation

March 2022

Scottish Public Sector Data Retention Rules

Government and other public sector organisations must delete data associated with FOI and EIR requests after 3 years. There is an exception for requests with a Review or Appeal which should be kept for 6 years.

DPA/SAR information requests should be deleted after the same periods but, at time of writing, this is being confirmed.

In addition, and in conjunction with the normal contact data cleaning functions which allow a deletion of individuals' data, some organisations would like the ability to delete individual IRs at will. AXLR8 can consider this enhancement but there are no plans at present to develop this. The reason is that there could be a risk an IR was deleted after, say 3 years when it had an appeal. Or it could be deleted without some other check

Definitions

Contact	A contact above normally means an applicant. It is a “person”.
Site	A Site is an address
Organisation	Normally a company (e.g. a newspaper) or public sector organisation but can also be a household in the case of a private individual applicant.
Attached file	Any attached document, spreadsheet, picture, scan that has been added to an IR, contact, or any entity on the system. Also referred to as a “fileattach”.
User	A User means someone with a log in =account on your AXLR8 system. Sometimes called an Employee (of your organisation).
Audit Data	The date and time stamped changes and which User was responsible
IR	IR stand for Information request and could be a Complaint, SAR, FOI or EIR or any other type of request on your system.
Feedback Requests	Those records created by the “self-service” forms on your website provided by AXLR8 or any where an IR has been auto-created using the AXLR8 email2IR function.
Filter Date	The latest of the closure date of the IR, the Review or the Appeal of each IR. For example, if your retention period is 3 years, the IRs will be filtered for those that are earlier than 2 years and 11 months ago and queued for the optional spot check (with recue opportunity) and auto deletion the following month.

Planning the Automation Process

Agree business rules

We will need to formally sign off the business rules as the destruction of the data is permanent. Then we will have a manual check process for two or three cycles in order to assure safety of data that must not be deleted.

Team

We need to formally agree who from your organisation has the authority to give AXLR8 directions and sign off the rules we implement and to whom we should address queries/

Testing manually

The challenge is to make sure we do not delete something we later need. This is because the whole design of the system historically has been to keep from losing data. The automated deletion / obfuscation processes delete data and files permanently. Please look carefully at the safety mechanisms in the business rules below to make sure you can allocate (a) competent officer(s) to work with them on a regular monthly basis. This officer/ team will need to check items flagged for deletion before the monthly process runs.

Please also see the “Implementation” section later in this document.

Several developments since 2017 have now created a good algorithm for what gets deleted and how you can check. It can be customised for your organisation and we feel it can still be improved in many ways so we welcome suggestions for future releases.

Hopefully, when reading the business rules below, you will we have thought through many of the questions you will be asking. For example, an applicant form a SAR 6 years ago should be deleted – but not if they have another SAR running currently. An IR may have been closed in January 3 years ago but a Reviews and Appeal take the closure date for that IR six months later hence escaping the deletion line.

See also “Back ups” section below.

What data?

The data to be deleted includes personal data (which may be deleted or obfuscated if still required for MI and Audit), Information Requests and associated Reviews and Appeals, Audit Trail, Files and attachments.

Business Rules

Here are the business rules. You may wish to change some of them to suit your organisation (e.g., change the timescales). Please read through them carefully and do not hesitate to call AXLR8 Support to speak to a consultant in more detail about your requirements.

Monthly data clean up automation based upon a historical “closure” date
 Here are the business rules translated as closely as possible from the code into “English”.
 Most clients agree a Monthly cycle is optimal but we suppose you could run it daily or weekly or any other cycle if you wish us to customise it. It is quite flexible. In future, if you want it to work with 4 years instead of 3 years, these parameters may be changed by our analyst programmers.

The system has evolved over the years and it now selects IRs (SARs, FOIRs, EIRs, etc.) on the **latest of the closure date of the IR, the Review or the Appeal of each IR.**

On each run cycle, the Monthly Clean Up process:

- 1) *Filters out those IRs with a Review or Appeal (for which 5 years and 11 months replaces 2 years and 11 months in “Filter Date” in the point below)*
- 2) *Calculates the date 2 years and 11 months ago (Filter Date) – thus giving you 1 month where we can restore.*
- 3) *Finds all information requests created on or before that filter date where.*
 - a. *The contact for the information request does not have another information request more recent than that filter date.*
 - b. *The contact has a related email address.*
- 4) *The information request is flagged to be deleted.*
- 5) *(Optional) The contact is flagged to be deleted if their email address is not the same as a related email address for an employee.*
- 6) *Process to delete contacts.*
 - a. *Deletes contact.*
 - b. *Deletes feedback entries for the contact.*
 - c. *Deletes orphaned organisations that were added before the filter date (ones that have no contacts on them – i.e. ones that have just been deleted).*
 - d. *Deletes orphaned sites (ones where the sites organisation does not exist).*
 - e. *Deletes all related email addresses for contacts that were previously deleted.*
 - f. *Deletes all email records for the contacts that were previously deleted.*
 - g. *Deletes orphaned org / site / contact lookups (where org / site or contact for the lookup is now deleted).*
 - h. *Deletes orphaned org / site / contact attached files (same as above).*
 - i. *Deletes orphaned org / site / contact notes (same as above).*
- 7) *Process to delete information requests.*
 - a. *Deletes information requests.*
 - b. *Deletes reviews for the IR’s it has just deleted.*
 - c. *Deletes orphaned activities (ones where their parent IR does not exist).*
 - d. *Deletes orphaned activity notes (ones where the activity does not exist).*
 - e. *Deletes all email links connected to the IR’s.*
 - f. *Deletes all emails that were connected to the IR’s (that were not connected to another IR that is not being deleted – e.g. leaves emails where the subject had two IR numbers and only one of them is being deleted – so the email has to stay as its related to the other IR).*
 - g. *Deletes orphaned lookups / attached files / notes for IR’s (where the IR does not exist).*
- 8) *Final clean up.*
 - a. *Deletes feedback entries created before the filter date where they are not connected to a contact.*
 - b. *Deletes any audit data on or before the filter date.*

Back ups

AXLR8 keep back ups of all your data. These are not immediately affected. They become progressively overwritten by the newly “pruned” database. Thus, a database where the “auto-clean-up” has deleted three people’s private data four days ago will have four back ups without those three people’s data and all earlier back ups will still retain those people’s private data until they are overwritten. For most clients we keep a back up every night for 30 days and then one a month is kept for historical diagnostics and security. Please inform us if you wish to shorten the retention period and we can do this but you must accept the entire responsibility if you subsequently discover you need something from two years ago or if AXLR8 are unable to diagnose a problem because we need to analyse (for example) the 2014 back up.

Implementation

Implementation requires scoping and customisation with your team and our consultant. We need to agree parameters and run some trials on a copy database to make sure the results are as desired. Following a feedback and snagging process we will ask your approval to do (at least) two similar monthly cycles on the live system. Clearly the first will be the biggest in volume and testing/analysis. When we are all comfortable with the test cycles, we will agree with you which day of the month the automation will run (e.g. 26th or last Friday of every month, etc.). By then we will also have agreed a prior inspection a couple of weeks before where your designated officers/ team may look at the data flagged for deletion and decide if there should be exceptions.

Costs

This is normally a couple of days consulting for AXLR8.