



EUROPE & SCOTLAND
European Regional Development Fund
Investing in a Smart, Sustainable and Inclusive Future



EUROPE & SCOTLAND
European Social Fund
Investing in a Smart, Sustainable and Inclusive Future

EUROPEAN STRUCTURAL AND INVESTMENT FUNDS

2014-2020 PROGRAMME

Document Retention Guidance

Document Retention Guidance

Revision History

Date	Issue	Change Made	Author
19/03/2019	0.1	Creation (draft)	I McNeil/ J Findlay
12/09/2019	0.2	Changes following PGG	I McNeil/ J Findlay
21/02/2020	0.3	Changes from POM and pre-PGG	Darren McDowall
04/03/2020	0.4	Changes from PGG	Darren McDowall
26/03/2020	0.5	Updates as requested by the Audit Authority	Darren McDowall
30/03/2020	1.0	Issue	Tracey Gillon

INDEX

Section 1 – Guidance for Lead Partner	Paras 1.0 – 1.7
Section 2 – Format of Documents	Paras 2.0 – 2.12
Section 3 – Third Party Document Retention	Paras 3.0 – 3.3
Section 4 – Further Document Retention Considerations and Requirements	Paras 4.0 – 4.10

1.0 Guidance for Lead Partner

- 1.1 The following guidance details the requirements of European Commission Article 140, EU regulation No 1303/2013.
- 1.2 Document and Record Retention Periods, unlike previous programmes, retention periods for Lead Partners are no longer linked to the Programme closure process, meaning that average retention periods will reduce.
- 1.3 In most cases, the retention period will be around 3 to 4 years following the end of each operation. However, the Managing Authority should be consulted where Lead Partners are unsure on document retention timescales as extended periods may be required, such as State Aid implications, audits or investigations.
- 1.4 For all operations, all supporting documents shall be made available for a two year period from 31 December following the submission of the accounts and subsequent audit period in which the final expenditure of the completed operation is included.
- 1.5 Lead Partners will be advised by the Managing Authority of the commencement of their retention period following payment of their Final Claim for individual operations.
- 1.6 It remains the responsibility of the LP to ensure that all Delivery Agents are informed of their requirements in relation to document retention following receipt of confirmation of retention dates from the MA.
- 1.7 This guidance does not supersede General Data Protection Regulations (GDPR), it is the Lead Partners responsibility to ensure full compliance with GDPR and all relevant Data Protection guidance. Further information on GDPR is available from Gov.uk and the Information Commissioner's Office.

2.0 Format of Documents

- 2.1 Documents can be retained in any of the following formats detailed below.
- 2.2 Documents that originate and exist only in their native digital form i.e. so-called 'born digital' records such as e-mails, database records, spreadsheets and word processing files etc. This extends to both structured and unstructured records, and includes, for example,
 - electronic records management systems;
 - digital file formats, such as PDF, JPEG and TIF when created and then transmitted digitally;
 - databases;
 - video clips,
 - Digital photography etc.

- Electronic/ digital versions of original paper documents held on commonly accepted data carriers such as microfilm, digitised/ scanned/ replica images etc.
- Original paper documents.

2.3 Certified true copies of an original paper document. [See article 140 of EU 1303/2013]. Conditions for accepting documents that originate in electronic/ digital form to ensure that the authenticity and integrity of 'electronic/ digital only' records so that they can be relied upon for legal and audit purposes, you must be satisfied that the ICT/ information management systems in place are designed to conform to accepted security standards in the UK.

2.5 You should obtain the relevant assurances on security standards from your ICT/ Information Assurance Officer or management team. This approach extends to seeking assurance on records held on the ICT systems of any joint beneficiaries or contracted/ third party deliverers holding documents electronically/ digitally.

2.6 For the purposes of our verifications and audits, you should keep a document that describes the procedures you have undertaken to obtain the necessary assurances that adequate security standards are in place to rely on the information held electronically/ digitally.

2.7 If you are unable to obtain the necessary assurances on the security standards, then the records will not be acceptable for EC/ Managing Authority compliance purposes [article 140(6) of EU 1303/2013].

2.8 Conditions for accepting digitised, scanned, replica digital versions of original paper documents:-

2.8.1 Lead Partners using scanning, e-archiving or image processing systems (where original paper documents are scanned and stored in digital form) must ensure that certification processes and controls are in place that, at least:

- Guarantee that each 'e-document' (scanned image) is identical to the paper original.

2.8.2 Prevent or detect the scanning of the same paper document to produce several different e-documents of the same original document (each e-document remains unique and cannot be re-used for any other than its initial purpose).

2.8.3 Where the document evidences a financial transaction, the approval, accounting and payment process for each e-document should be unique (it should not be possible to approve, account for, or pay the same e-document twice).

2.9 Once scanned, processes and controls prevent or detect the amendment of e-documents or the creation of altered copies (or amended/ altered versions are held as separate versions and the original, unaltered version of the image remains available for audit purposes).

2.10 Verifications and audits may ask to examine the policies and procedures in place to provide assurance of the above certification processes and controls, and may also ask to observe the scanning and certification process taking place in real time.

2.11 Where originals are not retained, certified true copies of original paper documents (photocopies) can be used, but should comply with best practice:

2.11.1 The photocopied document must contain a 'certification statement'. The certification declaration must be annotated on, or appended to, the copy. The original document does not need to be marked.

2.11.2 If a document contains multiple pages then the first page should be certified and the number of attached pages indicated on the front page (alternatively, each page could be certified).

2.11.3 The certification statement must be authorised/ signed and dated by an employee who can vouch that the copy is a true replica image of the original.

2.11.4 The certification statement is added at the time that the copy is made. Alternatively, the certification statement can be added shortly afterwards if the signatory can recall seeing the original and is therefore still able to confirm that the copy is satisfactory.

2.11.5 The 'certification statement' can be chosen by each Lead Partner but must, at least, contain the following:

- Signature [or similar evidence of authorisation]
- Date
- 'True copy', 'certified copy', 'certified' [or similar phrase to signify what the signature and date represents]

2.11.6 It is recommended, but not mandatory, that the certification statement also includes the printed name/ position of the signatory or other unique reference (such as employee/ payroll number) so that future project staff and/or auditors are able to easily identify the signatory if required. The following is an example of a compliant certification statement:

I, *Name of person certifying*, certify this document as a true copy of the original

Signature:

Date:

Position:

Name of Organisation:

Number of Pages Certified:

2.11.7 If more efficient, a single certification declaration can be used for a batch of photocopies. The certification statement must include:

- A unique batch reference number/ code to identify the batch.
- The number of documents – and pages if individual documents contain more than one page – included in the certified batch.
- The references/ numbers of each of the documents included in the batch. If the documents are not already referenced/ numbered, then references/ numbers should be added to each document prior to batch certification.

2.12 Where originals are not retained, and best practice as outlined is not followed, the Managing Authority reserves the right to assess the processes and procedures of the organisation to determine whether sufficient assurance of document authenticity is provided. Expenditure may be deemed ineligible if document authenticity cannot be verified.

3.0 Third Party Document Retention

3.1 Records and Documents not held on the Lead Partners Premises

Accounting records and supporting documents could be held by:

- Lead Partner (Lead Partner or Delivery Agents); or
- Third party delivery partners such as procured contractors/ service providers.

3.2 Where records are held at locations other than The Lead Partners premises – such as off-site storage facilities or the premises of partners and service providers/ contractors – then The Lead Partner must satisfy themselves that storage is in line with the expectations of this guidance, such as:

- Records are retrievable and accessible;
- Partners/ providers allow full access to records at their premises, including where applicable, access to view 'born digital' or digitised records using a suitable ICT device or workstation; and
- Records are complete; structured and well-organised; in good condition; and
- In an acceptable format that meets MA requirements.

3.3 In the absence an adequate audit trail, or the inability to access records during audits and verifications, this could lead to the associated expenditure being declared as ineligible with a corresponding reduction in EU grant, whether the problems arise through the Lead Partners own actions, or that of a partner/provider.

Examples of Good Practice for third party document retention management include, but are not limited to:

- A record of regular spot-checks performed on partner organisations, including details of any remedial action taken when the results of the spot-checks prove unsatisfactory.
- Where it is clear that partners/ providers are not able to satisfy these standards, all records are transferred and held by The Lead Partner.

- Where the Lead Partner considers it necessary, they should also consider requiring the transfer of original documents at the time that Delivery Agents/ providers submit their invoices or expenditure declarations.
- Photocopies, scanned images and digital records held by partners/ providers remain subject to the usual safeguards on authenticity.
- Similarly, where The Lead Partner is informed, or suspects, that a partner/ provider may shortly cease trading (close down, dissolved, liquidation etc.) or other imminent event that may impair the ability to comply with all record-keeping requirements, it must arrange for the records to be transferred and held at its own premises.

4.0 Further Document Retention Considerations and Requirements

- 4.1** When deciding on the most appropriate document format, please remember that records may need to be retained for a longer period than your normal organisation records retention policy requires.
- 4.2** You may need to label and store EU project records to prevent their premature destruction.
- 4.3** You will also need to consider practical issues such as storage space and the risk of damage or technological obsolescence.
- 4.4** You should give particular consideration to the risk of technical obsolescence of digital records, both the ICT hardware or software applications used to access the records.
- 4.5** Organisations holding records will need to ensure that original records are retrieved from all electronic records systems that risk becoming obsolete or no longer accessible.
- 4.6** To be clear, there is no expectation or requirement by The Managing Authority or the European Commission that hard-copy documents or 'wet signatures' must be used or are preferable to digital records. Indeed, the EC and The Scottish Government fully encourage beneficiaries to maximise the opportunities to embrace the benefits of paperless administration, where appropriate certification, as outlined previously is followed. Where electronic signatures and documentation are used and submitted via the EUMIS system, this is acceptable. Where documentation is not submitted via EUMIS, it must be received from an official email address within the LP organisation, and copied to a designated signatory.
- 4.7** Lead Partners should therefore note the guidance in Section 2 above and consider how technology can provide suitable methods to, for example, identify and authenticate a document, or demonstrate the authorisation of a transaction, information or decisions.

- 4.8** All records must be readily accessible for audits, verifications and any related investigations.
- 4.9** We will aim to provide you with as much notice as possible when we need to examine project records but, particularly as the EC is only required to provide 12 working days' notice for their audits, you should ensure that arrangements are sufficiently robust to cater for such requests.
- 4.10** If records are unavailable during visits, related expenditure could immediately be declared as ineligible.