Data Protection Policy

Contents

Purpose of the policy

Heart of England Community Foundation (HoECF) needs to gather and use certain information about individuals. These can include employees, volunteers, contractors, service providers, individuals linked to grant applicants and grant recipients, individuals linked to potential grant applicants, donors, potential donors, supporters, ambassadors and other stakeholders. This list is not exhaustive.

This policy describes how personal data must be collected, handled and stored to meet the charities data protection standards — and to comply with the privacy and data protection laws including:

a) The General Data Protection Regulation (the GDPR) and any related legislation which applies in the UK, including any legislation derived form the Data Protection Bill 2017;

b) The Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including E-Privacy Regulation 2017/0003;
c) All other applicable laws and regulations relating to the processing of personal data and privacy, including the guidance and codes of practice issued by the Information Commissioner's Officer (ICO) and the Fundraising Regulator.

This policy exists to ensure that HoECF:

a) Complies with the legislation listed above and follows good practice
b) Protects the rights of all individuals where we process their personal data
c) Is open about how it stores and processes individuals' data
d) Protects itself and individuals where we process their personal data from the risks of a data breach.

This policy is supported by the *Privacy Notice* that sets out how we process data on individuals.

This policy covers all types of personal data relating to the categories of individuals listed above. The Operations Manager is the Data Protection Officer at HoECF and is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to the Data Protection Officer.

Anyone who handles personal data on behalf of HoECF including employees and volunteers, must comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

Scope

This policy applies to:

a) The head office of HoECF
b) All branches of HoECF, including Community Matters
c) All staff and volunteers of HoECF, including trustees
d) All contractors, suppliers and other people working on behalf of HoECF.

It applies to all personal data and sensitive personal data as defined in Section 4 below. Further guidance on how to identify what is personal data and examples of personal data and sensitive personal data are provided in Appendix A.

Responsibilities

The key areas of responsibility are as follows:

The Board of Trustees is ultimately responsible for ensuring that Heart of England Community Foundation meets its legal obligations.

The Data Protection Officer is responsible for:

a) Keeping the CEO and board updated about data protection responsibilities, risks and issues
b) Reviewing all data protection procedures and related policies, in line with an agreed schedule
c) Arranging data protection training and advice for the people covered by this policy.
d) Handling data protection questions from staff and anyone else covered by this policy
e) Dealing with requests from individuals to see the data Heart of England Community Foundation holds about them (also called 'subject access requests')
f) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data. Ensuring all systems, services and equipment used for storing data meet acceptable security standards
g) Instructing regular checks and scans to ensure security hardware and software is functioning properly
h) Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services. Approving any data protection statements attached to communications such as emails and letters.
i) Addressing any data protection queries from journalists or media outlets like newspapers
j) Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Definitions of data protection terms

The following terms will be used in this policy and are defined below:

Data Subjects include all living individuals about whom we hold personal data, for instance an employee or donor. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data (which is defined as "special categories or personal data" under the GDOR) includes information about a person's:

a) Racial or ethnic origin
b) Political opinions
c) Religious, philosophical or similar beliefs
d) Trade union membership
e) Physical or mental health condition
f) Sexual life or orientation
g) Genetic data

h) Biometric data.

Data Controllers are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation above. HoECF is the data controller of all personal data that we manage in connection with our work and activities.

Data Processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

ICO means Information Commissioner's Officer (the authority which oversees data protection regulation in the UK)

Processing is any activity that involved use of personal data, whether or not by automated means. It includes:

a) Collecting
b) Recording
c) Organising
d) Structuring
e) Storing
f) Adapting or altering
g) Retrieving
h) Disclosing by transmission
i) Disseminating or otherwise making available
j) Alignment or combination
k) Restricting
l) Erasing
m) Destruction.

Data Protection Principles

Any one processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles and show that we comply, in respect of any personal data that we deal with as a data controller.

Personal data should be:

a) Processed fairly, lawfully and transparently
b) Collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes
c) Adequate, relevant and limited to what is necessary for the purpose for which it is held

d) Accurate and, where necessary, kept up to date
e) Not kept longer than necessary
f) Processed in a manner that ensures appropriate security of the personal data.

Processing data fairly and lawfully

The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent or where the processing is necessary for one or more specified reasons, such as where is it necessary for the performance of a contract or where the charity has a legitimate interest in processing that data.

To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we will provide that person with "the fair processing information". In other words, we will tell them:

a) The type of information we will be collecting (categories of personal data concerned)
b) Who will be holding their information, i.e. Heart of England Community Foundation including our contact details, and the contact details of our Data Protection Officer
c) Why we are collecting their information and what we intend to do with it, for instance to process donations or send them mailing updates about our activities
d) The legal basis for collecting their information (for example, because they have given their consent or because we have a legitimate interest)
e) If we are relying on legitimate interests as a basis for processing, what those legitimate interests are
f) Whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not proving that data
g) The period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period
h) Details of people or organisations with whom we will be sharing their personal data
i) If relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards
j) The existence of any automated decision-making, including profiling in relation to that personal data.

Where we obtain personal data about a person from a source other that the person his or her self, we must provide that individual with the following information in addition to that listed above:

a) Categories of personal data that we hold
b) The source of the personal data and whether this is a public source.

In addition, in both scenarios (where personal data is obtained both directly and indirectly), we must also inform individuals of their rights, including the right to lodge a complaint with the ICO, and the right to withdraw consent to the processing of their personal data.

This fair processing information can be provided in a number of places including on web pages, in mailings or on applications forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

Processing data for the original purpose

The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities, it should not the be used for any new purpose, for example, to share with other organisations for marketing purposes, without first getting the individual's consent.

Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

Not retaining data longer that is necessary

The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date data or inaccurate personal data, please contact the Data Protection Officer.

See Appendix B for details of retention periods relating to specific types of data, including statutory retention periods.

Data collected as part of the Community Matters project, part of the Building Better Opportunities programme funded by the Big Lottery Fund and European Social Fund will be retained in line with ESF rules as summarised in Appendix C.

Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of HoECF need to be aware of these rights. They include the right:

a) To request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights)
b) To be told, where any information is not collected from the person directly, any available information as to the source of the information
c) To be told of the existence of automated decision-making
d) To object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests
e) To have all personal data erased (the right to be forgotten) unless certain limited conditions apply
f) To restrict processing where the individual has objected to the processing
g) To have inaccurate data amended or destroyed
h) To prevent processing that is likely to cause unwarranted substantial damage or to distress to themselves or anyone else.

Data security

The sixth data protection principle requires that we keep secure any personal data that we hold.

This section details the procedures we have in place to ensure that personal data is held securely including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure.

When we are dealing with sensitive personal data, more rigorous security measures are used.

The majority of the personal data and sensitive personal data used by HoECF is held:

- Salesforce – web-based record management system
- Evolutive – web-based record management system
- Shared Drive
- In paper files held at the Coventry office and the Dudley office.

The procedures we have in place for the protection of data held in these locations include:

- Both Salesforce and Evolutive require each individual user to have a username and password
- Permissions within Salesforce and Evolutive are restricted based on the requirements for each individual employee in relation to their job role

- Each employee is required to have a username and password to log in to their work computer account, employees are required to change these passwords on a regular basis
- Individuals cannot access our Shared Drive without an employee account with a username and password
- Permissions within the Shared Drive are restricted based on the requirements for each individual employee in relation to their job role
- Our Shared Drive is backed up remotely, ensuring that we will be able to retrieve the data held if our servers were not available
- The data on Salesforce and Evolutive is held remotely and not dependent on the charity's servers
- Sage
- All servers and computers are protected by approved security software and a firewall
- Paper files containing personal data and sensitive personal data are kept in locked cupboards or drawers
- Paper files may be stored securely in an offsite location owned and managed by a third party. HoECF will ensure that data held in these locations is only accessible to HoECF employees and appropriately security vetted employees of the third party. HoECF will also ensure that files are accessible at short notice if required, for example when an audit is taking place.
- Personal data should not be transferred by email unless strictly necessary. If personal data is transferred by email, it needs to be adequately protected such as an encrypted attachment.

Additional specific procedures relating to the Community Matters project, part of the Building Better Opportunities programme funded by the Big Lottery Fund and European Social Fund:

- Any personal data or sensitive personal data that is transferred to HoECF from partner organisations needs to either be delivered by hand by an employee of the partner to an employee of HoECF (it should not be put through the letter box or to an employee of Summit House) or saved securely on One Drive.
- Any personal data or sensitive personal data that is transferred from HoECF to the Big Lottery Fund needs to either be shown to a duly authorised employee of the Big Lottery Fund or uploaded securely through the Kiteworks system.

When working from the office, all employees are required to:

- Ensure that individual monitors do not show confidential information to passers-by
- Ensure any conversations that include discussion of personal data are held in a private location such as a meeting room
- Either lock their screen or log off from their computer when it is left unattended
- Set a passcode for any work mobile phones
- Clear their desk of any confidential paperwork if they are leaving their desk unattended
- Keep all confidential information held in paper format in locked desk drawers or cupboards
- Ensure that any lockable office doors are kept locked if the office is unattended
- Lock away any removable storage devices (such as Memory Sticks) when not in use or left unattended.

When working away from the office, all employees are required to:

- Ensure that laptops and mobile phones are with them at all times, for example they should not be left in a car during meetings or overnight
- Keep removable storage devices with them at all times
- Try not to take any paper copies of confidential information out of the office unless strictly necessary, or if necessary to ensure these documents are with them at all times.

Transferring data outside the EEA

GDPR requires that when organisations transfer personal data outside the EEA that they take steps to ensure that the data is properly protected.

The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but this list may be updated. As such personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA.

The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the Data Protection Officer before transferring personal data to organisations in the US.

Through the use of Salesforce, it may be that some personal data is transferred to the US. Working with UKCF who hold the agreement with Salesforce on behalf of a number of community foundations, HoECF has ensured that appropriate security procedures are in place to protect this data. For more information, please speak to the Data Protection Officer.

For the purposes of clarity, no personal data or sensitive personal data processed for the Community Matters project will be transferred outside the EEA.

Processing sensitive personal data

On some occasions we may collect information about individual that is defined by the GDPR as special categories of personal data and special rules apply to the processing of this data. In this policy we refer to “special categories of personal data” as “sensitive personal data”. The categories of sensitive personal data are set out above.

Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

In most cases, in order to process sensitive personal data, we must obtain explicit consent form the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to the Data Protection Officer.

Notification

We recognise that while there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the UCO where necessary when we are carrying out “high risk” processing.

We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

All employees are required to notify the Data Protection Officer and the CEO of any potential data breaches at the earliest possible opportunity regardless of their severity. This could include for example and email being sent to a contact list using cc instead of bcc (where recipients can see the email addresses of all other recipients) or the loss of work mobile phone or laptop.

Appendix A

(from 'Determining what is personal data – quick reference guide' www.ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf)

Is the information 'personal data' under GDPR?

1.	**Can a living individual be identified from the data, or, from the data and other information your possession, or likely to come into your possession?**	
	Yes	Go to question 2.
	No	The data is not personal data for the purposes of the

2.	**Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?**	
	Yes	The data is 'personal data' for the purposes of the DPA.
	No	The data is not 'personal data' for the purposes of the DPA.

3.	**Is the data 'obviously about' a particular individual?**	
	Yes	The data is 'personal data' for the purposes of the DPA.
	No	Go to question 4.

4.	**Is the data 'linked to' an individual so that it provides particular information about that individual?**	
	Yes	The data is 'personal data' for the purposes of the DPA.
	No	Go to question 5.

5.	**Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?**	
	Yes	The data is 'personal data' for the purposes of the DPA.
	No	Go to question 6.

6.	**Does the data have any biographical significance in relation to the individual?**	
	Yes	The data is likely to be personal data for the purposes of the DPA.
	No	Go to question 7.
	Unsure	Go to question 7.

7.	**Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?**	
	Yes	The data is likely to be personal data for the purposes of the DPA.
	No	Go to question 8.
	Unsure	Go to question 8.

8.	**Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?**	
	Yes	The data is 'personal data' for the purposes of the DPA.
	No	The data is unlikely to be 'personal data'.

Examples of personal data:

- Name
- Date of birth
- Personal phone number
- Personal email address
- Personal postal address
- Job title and employer
- Business phone number
- Business email address
- Business postal address
- Details of volunteer, trustee or director roles
- Details of Facebook page
- Twitter handle (username)
- Details of LinkedIn page
- Bank account number and/or sort code.

Examples of sensitive personal data:

a) Racial or ethnic origin
b) Political opinions
c) Religious, philosophical or similar beliefs
d) Trade union membership
e) Physical or mental health condition
f) Sexual life or orientation
g) Genetic data
h) Biometric data.

Appendix B

Statutory Retention Periods

Record	Statutory Retention Period
Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos)
Accounting records	3 years for private companies, 6 years for public limited companies
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate
Records relating to children and young adults	Until the child/young adult reaches the age of 21
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends
Wage/salary records (also overtime, bonuses, expenses)	6 years
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover
Records relating to working time	2 years from date on which they were made

Other Retention Periods

These retention periods are subject to variation:

Record	Recommended Retention Period
Application forms and interview notes (for unsuccessful candidates)	1 year
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently

Inland Revenue/HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after benefit ceases
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Senior executives' records (that is, those on a senior management team or their equivalents)	Permanently for historical purposes
Statutory Sick Pay records, calculations, certificates, self-certificates	The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.
Fund holder agreements	6 years from the date the agreement ends.
Board minutes, committee meeting minutes	Permanent
Panel meeting minutes	Permanent
Grant applications	Permanent
Details of grant recipients and grant agreements	Permanent
Details relating to donations	6 years

Appendix C

Taken from Guidance on *Document Retention, including Electronic Data Exchange, for 2014-20 Projects* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591617/ESF_Guidance_on_document_retention.pdf (as at 19th January 2018).

DOCUMENT RETENTION, INCLUDING ELECTRONIC DATA EXCHANGE FOR 2014-20 ESF PROJECTS

Introduction

1. As stated in the ESF Funding Agreement, ESF grant recipients are required to provide records to evidence that the expenditure in claims complies with the relevant regulations, rules and terms of the Funding Agreement, to enable the Managing Authority to meet its reporting obligations and to demonstrate compliance with EU requirements.

2. Good record keeping is an essential project management tool. By keeping orderly and comprehensive records, grant recipients will find it far easier to assess and report on the project status and progress in monitoring the project.

3. Record retention is an important consideration in the development and delivery of a project funded by ESF. Projects can be subject to an audit even after the project is completed and it is therefore a requirement of grant that core documents are retained and made available for inspection over the entire period. Failure to produce adequate and satisfactory evidence can result in the repayment of grant.

4. To ensure that this process is followed, all applicants are required to produce and provide as evidence, policies for specific areas including document retention. This reference can be included in current policies that the grant recipient already uses or separate policies specifically developed for the ESF project to follow.

5. For projects delivered by a consortium of partners, it is the Grant Recipient organisation that is responsible for the audit trail. The Grant Recipient must make sure that any delivery partners or sub contractors keep adequate records. To do this, they will need to show that they have systems in place to verify the information provided and held by partners.

How long do records need to be kept?

6. All projects are required to retain documents for a period after the activity has ended and these should be kept in an acceptable format so that they can be inspected where necessary. The grant recipient will be informed of this retention period at the end of the project. The period is dependent on the date at which the final claim is submitted to the Managing Authority so the retention period will be unique to each project and this period cannot be specified at the outset.

7. As a minimum, all documents must be retained for two years after the Audit Authority submits the Annual Control Report in which the final expenditure for

the completed project is included. This should not be interpreted by grant recipients as two years after the project submits its final claim. This is to ensure documents may be made available to the European Commission and European Court of Auditors upon request in accordance with Article 140(1) of Regulation (EU) No 1303/2013.

8. In addition to this rule grant recipients must comply with and assist the Managing Authority to comply with document retention requirements under any applicable State Aid rules. Where Projects are operating under a State Aid scheme in accordance with the General Block Exemption Regulation (Commission Regulation (EU) No 651/2014) or De Minimis Regulation (Commission Regulation (EU) No 1407/2013), Grant Recipients must maintain detailed records with the information and supporting documentation necessary to establish that all the conditions laid down in the Regulation are fulfilled. Such records must be kept for 10 years after the last aid is granted under the scheme.

9. Prior to the destruction of any documents, confirmation should be sought from the Managing Authority.

What documentation should be retained?

10. Core documentation that must be retained will include:

- all ESF related documentation including work carried out during the development, pre application, application and during and after the project;
- the Funding Agreement including any revised versions supported by appropriate correspondence from DWP of the approval of changes to the Funding Agreement;
- correspondence from/to the Managing Authority;
- quarterly or monthly claim forms;
- working papers showing how claims were calculated, including any flat rate methodologies;
- the audit trail for all procurement undertaken for the project; and
- the State Aid approved scheme used where relevant.

11. You must keep records of the following things although this list is not exhaustive:

- evidence of all project expenditure. This must include invoices and bank statements or equivalent to show the payments were made;
- where indirect overheads costs and salaries have been apportioned to the project, records must show the agreed methodology for calculating these costs;

- records of eligible beneficiaries and any supporting evidence to confirm their eligibility to receive ESF support;
- evidence of open and fair procurement of goods and services. Including proof of advertising and contract notices, quotations or tenders received and the scoring methodology used for selecting the successful candidate. This will include details of all preparatory work prior to the procurement process and the delivery/use of the procured service and goods. See The National Procurement Guidance on https://www.gov.uk/england-2014-to-2020-european-structural-and-investment-funds for further information on procurement requirements;
- evidence of auditable, accountable match funding, including copies of match funding acceptance letters and bank statements showing receipt of match funding;
- compliance with publicity requirements. Copies of all publicity materials, including press releases and marketing must be retained to demonstrate the correct use of the EU logo and required text. See ESF Publicity Requirements, also on the above website, for further information on publicity requirements;
- compliance with equal opportunities and environmental sustainability requirements;
- clear records of businesses supported for state aid purposes, including signed declarations where an organisation is operating under any state aid rules, such as de minimis, or any other state aid ruling;
- documentary evidence substantiating the outputs and results declared in ESF claims and on completion of projects;
- a record of the identity and location of all bodies holding the supporting ESF project documentation and make this available on request to the Managing and Audit Authorities.

Electronic data exchange - legislative requirements

12. Commission Implementing Regulation (EU) No 1011/2014, Chapter II sets out the detailed rules concerning the electronic exchanges of information between beneficiaries and Managing Authorities, CAs, AAs and Intermediate Bodies.

13. Article 8 of the Regulation defines electronic data exchange systems as mechanisms and instruments allowing the electronic exchange of documents and data, including audio-visual media supports, scanned documents and electronic files. This exchange shall include reporting on progress, payment claims and exchanges of information related to management verifications and audits. Paper documents may only be requested by the MA, CA or AA in exceptional cases, following a risk analysis, and only if paper documents are the true source of the scanned documents uploaded in the electronic data exchange system.

14. The ESIF E-Claims system has been designed to comply with electronic data exchange systems requirements and will have the following functionalities:-

    - interactive forms and/or forms prefilled by the system on the basis of the data which are stored at consecutive steps of the procedures;
    - automatic calculations where applicable;
    - automatic embedded controls which reduce repeated exchanges of documents or information as far as possible;
    - system-generated alerts to inform the beneficiary that certain actions can be performed;
    - online status tracking allowing the beneficiary to monitor the current status of the project;
    - availability of all previous data and documents processed by the electronic data exchange system.

Acceptable forms of documentation

15. Electronic document storage systems are therefore acceptable, indeed necessary, as most documents now are electronically generated and have no paper original and will need to be made available through the electronic data exchange system. They are acceptable as audit evidence, provided that they are subject at all times to an adequate system of control over their completeness and validity. These systems of control may be subject to audit so that assurances can be obtained in this respect.

16. Documents can be held either as originals or certified true copies of the originals, or on commonly accepted data carriers. Commonly accepted data carriers include electronic versions of original documents on optical data carriers and documents existing in electronic version only.

17. Grant recipients should ensure that information kept on commonly accepted data carriers is kept secure and can be relied upon for audit purposes. As most documents exist in electronic version only, the underlying computer system on which the electronic versions are held must meet accepted security standards which ensure that the documents held meet with national legal requirements and can be relied upon for audit purposes. All electronic documents also need to have the equipment/software retained, to ensure it is functional for a two year period from 31st December following the submission of the annual accounts in which the final expenditure of the completed project is included.

18. Each version must be certified as conforming to the original document. A declaration by the grant recipient along the lines of the example below will satisfy this condition.

I certify that this is a true copy of the original document:

Signed

Date

Position in organisation

Name of organisation

19. This is the minimum requirement and grant recipients may add to this declaration or include additional procedures in line with their organisations policies should they wish to do so.

20. This minimum certification procedure places the onus on the grant recipient for ensuring the authenticity of the electronic copy. It is the grant recipient's responsibility to ensure the document can be retrieved and relied upon for audit purposes.

21. In instances where the grant recipient organisation is using an electronic Document Management System which involves the scanning of invoices and other documentation at the point of receipt, it is acceptable for the processes outlined above to be undertaken at the initial point of scanning by either the grant recipient or a third party acting on behalf of the organisation provided that the applicant organisation is satisfied with the procedures in place at the 3rd party organisation.

22. All electronic documents must be kept for the same duration as required for paper copies.

23. Exchanges of data and transactions should bear an electronic signature compatible with Directive 1999/93/EC on a community framework for electronic signatures. This will be provided by the DWP electronic data exchange system.