General Data Protection Regulation (GDPR) Policy 2023-2024

Version 2
Review Date: 07/06/2023
Next Review Date: 07/06/2024
Responsibility: Envisage Managers & Staff

Envisage Policy Statement

General Data Protection Regulation (hereafter referred to as 'GDPR') replaces the previous UK Data Protection (1998) by adopting Europe wide data protection guidelines that impact and have responsibilities for all government departments and agencies, businesses, social institutions and private citizens. There are a number of important changes and new obligations to be aware of that include increased protection and accountability of processing personal data, especially with regard to the security and storage of online data within the European Union.

This Envisage GDPR Policy includes actions that promote accountability and governance throughout the organisation. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's requirements emphasis elevates their significance. Organisations, such as Envisage are expected to put into place comprehensive but proportionate governance measures such as privacy impact assessments and privacy by design which are now legally required in certain circumstances where sensitive personal data is being requested and held by any organisation. Ultimately, these measures should minimise the risk of data breaches and uphold the protection of personal data.

Policy Objectives

This GDPR Policy will seek to:

- Define how Envisage and Envisage staff ensure compliance with the requirements of the General Data Protection Regulations (2018).
- It will identify appropriate processes and procedures for enabling compliance and transparency.
- Outline responsibilities to Envisage management and staff to ensure compliance.
- Provide guidance to learners, customers, partners, stakeholders and the general public on how Envisage will process requests and commit to respond to Freedom of Information (FOI) and 'right-to-erasure' requests.

ICO Registration

The GDPR stipulates a requirement for applicable organisations to hold valid registration with the Information Commissioner's Office (ICO). Envisage has registration with the ICO:

Envisage ICO Registration: ZA556572 Expiry Date: 13 October 2023

Data Protection Officer

The GDPR states that an organisation must appoint a Data Protection Officer (DPO) if they:

- Are a public authority (except for courts acting in their judicial capacity);
- Carry-out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- Carry-out large scale processing of special categories of data or data relating to criminal convictions and offences.

Envisage has identified the need for a DPO, who has an appropriate standard of expertise and will undertake appropriate training as deemed appropriate.

The DPO will operate as the lead in data protection for the organisation and be responsible for ensuring the compliance of the organisation with the GDPR – and reporting of potential breaches of compliance.

- Envisage's Data Protection Officer (DPO)**: David Ireson – Envisage Owner**

Why does Envisage collect personal data?

We collect details and information from our learners in order to ensure eligibility for their chosen training programme, register them for the qualifications they are working towards, maintain contact with them throughout their learner journey and ensure the best possible experience and outcome for them by screening for any special requirements they may have. We also collect personal data and information to ensure Envisage staff can provide accurate and appropriate Career Information, Advice and Guidance (CIAG) for learners that includes special categories of personal data or criminal conviction and offences data.

What personal data do we collect?

- Personal details as required by the awarding organisation.
- Evidence of eligibility for the training programme
- Screening for health and learning support
- Any criminal conviction and offences that may restrict or bar career progression or customer contact within the Exercise, Health and Well-being sector
- Contact details.
- Records of progress and achievement

How long do we keep personal data for?

- For self-funding learners, we destroy/delete all data after 3 years.
- For funded learners we keep everything required by the funding agency for the required length of time; this may vary according to the funding agency and the type of funding involved.
  - **Envisage Student Loan Company hard copy & digital learner personal data must be retained for six years (6) after the learner's last funding claim.**
  - **For the ESF 2014-2020 funding round; all Envisage ESF learner hard copy data must be retained to 31/12/2030.**

When do we use personal data to contact our customers?

Once learners have successfully completed their qualification and they have received their certificate, we would normally not contact them again unless they have indicated that they would like to join our marketing and mailing list. We ask all learners about this at the end of their course on our course evaluation form.

For learners that indicate that they do wish to be contacted, we only use the email provided on this form, all other personal data would be destroyed/deleted as normal after 3 years and they are able to unsubscribe from our mailing list at any time.

Statutory funding organisations may require Envisage to contact previous learners as part of a validation or quality assurance process; this would normally be within 12 months of completing a funded learning course.

Which statutory, partner and funding organisations do we share data with?

- YMCA Awards http://www.ymcaawards.co.uk
- ESFA Learner Records Service https://www.gov.uk/education/learning-records-service-lrs
- ESFA Employer Data Service https://edrs.education.gov.uk
- Student Loan Company https://www.lpservices.slc.co.uk/

GDPR Compliance

Article 5 of GDPR sets out seven key principles which lie at the heart of the general data protection regulation framework.

- Article 5(1) requires that personal data shall be:
  a. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
  b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
  c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
  e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
  f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
- Article 5(2) adds that: "The controller (Envisage's DPO) shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

  Envisage will ensure that in direct accordance to Article 5(2) that all personal data is:

  - collected ('processed') only where appropriate and with the explicit consent of the affected individual ('data subject') and only where required.
  - retained only for so long as is required (as outlined within the consent given by the individual at the point of capture)
  - subject to the legally defined rights of the individual to access, amend, erase and restrict processing of data relating to them.

The following sub-sections will detail how these points are addressed by the organisation, but in the case of any query or clarification being required, the appointed Data Protection Officer (DPO) should be contacted

Learner and Customer Data Processing

Envisage will follow GDPR requirements on the processing of customer and learner sensitive and personal data processed:

- Envisage and our staff will communicate clearly the purpose of the customer and learner data that is required to be collected from the each 'data subject'

- Ensure that the purpose in collecting and processing any data meets with GDPR legal data collection requirements;
  - To enable an individual or an organisation to work with Envisage to deliver Education and Training through a bilateral contract, based upon Envisage services and/or enable individual or organisation delivery needs through a contract for services.
  - Enable each party to meet all legal obligations
  - Ensure the individual's or organisation's key interests are met through services provided by Envisage (e.g., to protect their life)
  - Enable the completion of official functions in the public interest.
  - Resolve the requirements of legitimate partners, such as a funding, a third party
- Ensuring that all personal/sensitive data is only collected with the explicit written consent of the learner or organisation;
  - Learners and organisations are clearly informed of the valid necessity of data collection
  - Learners and organisations (authorised signatories) provide signed consent for the collection of personal/sensitive data
  - All evidence of signed consent is retained and can be revoked by an individual or an organisation through a documented process.

These data processing requirements and guidelines apply to all Envisage staff and associates, with any non-compliance by staff or associates potentially resulting in the instigation of investigation and/or disciplinary action by Envisage.

Data Retention

Envisage will abide by GDPR requirements and retain personal or organisational data;

- no longer than required for the identified purposes at point of processing
- ensure that the accuracy of the data is maintained whilst retained
- That all personal or organisational data is erased or anonymised (if used for analysis, it no longer be considered as 'personal' data) after it has been processed in accordance with GDPR
- Envisage may be required by legal and funding obligations to retain personal and organisational data for long periods after Education and Training activities/services in relation to; g periods due to 'long-term' purposes behind retention. These purposes include:
- Awarding body registration and ESFA/ESF/Student Loan Company contractual funding compliance (learners and employer organisations)
- For marketing and sales usage with anonymised or with permission from learners or organisational to use their data (working with funding partners and stakeholders)
- Financial and funding accounts and invoicing in respect of learners and organisations (working with funding partners and stakeholders)

Envisage will maintain and secure store all personal that is retained for funding and compliance requirements. It will be disposed of securely upon the legally required retention period has been met.

All Envisage staff process, report and monitor personal and organisational data and the subsequent sage storage of the data within Envisage's Information Security Guidelines. These guidelines outline;

- How personal learner and organisational data is retained and stored securely online or as hard data copy at Envisage premises.
- The retention periods applicable to different formats of data (as defined by the intended processing requirements)

Document and Digital Data Retention

The documents and digital records retained by Envisage will be managed as shown in the tables below:

Accounts	**Retention Period**
All records	6 years, unless ESF – 31/12/2030
Summary accounts	Indefinitely

Health and Safety	**Retention Period**
Completed accident forms & f2508 [RIDDOR] forms	indefinitely

Learner information – self funding	**Retention Period**
Personal details	Max 3 years unless additional permission for marketing is agreed
Registrations	Max 3 years
Assessment results	Max 3 years
Qualification or unit achievements	Max 3 years

Learner information SLC & ESF funding	**Minimum Retention Period**
Personal details	**Envisage Student Loan Company (SLC) digital & hard copy data kept by Envisage for 6 years, ESF hard copy data must be kept to 31/12/2030**
Additional information required by funding body	**As above with Personal Details**
All reports relating to learner journey	**As above with Personal Details**
Registrations	**As above with Personal Details**
Assessment results	**As above with Personal Details**
Qualification or unit achievements	**As above with Personal Details**

The above information will not be shared with third parties other than YMCA (awarding body), the ESFA, The Growth Company and the Student Loan Company as appropriate.

Other	
Learner images and testimonials	Permission is obtained for usage from the learner and/or employer for 5 years.

Learner and Employer Rights

Learner and Employer legal rights related to their personal data are protected by Envisage unless there are a legal basis for a disclosure. These rights relate to:

- be informed of personal data held by the organisation (a 'Freedom of Information' request)
- request access their personal data held by Envisage
- request to update and correct any personal data held by Envisage
- request the erasure personal data held by Envisage
- limit the manner in which their personal data may be processed by Envisage
- restrict how their data may be shared by Envisage
- object and withhold the processing of their data by Envisage

Though Envisage will respect and adhere to the legal rights of the learner and employer for any of their request around their data rights, the legitimate rationale for Envisage processing personal or organisational data, and any temporary retention of their data may mean that Envisage may be unable to fully comply with the requested action, as it may be contractually used or legally required by a government agency or approved government contractor.

This would not be the case for a commercial learner or customer, where Envisage can meet any data request or from a personal or organisation pertaining to an education and training activity or service that has been procured from Envisage.

Once the authorisation by the learner to share data has been signed by the learner or employer to share data with an approved awarding body, a government agency or a government authorised funding contractor/organisation, Envisage may be unable to comply with a learner or employer's request pertaining their data rights.

Envisage's primary basis for being unable to comply would be where undertaking of a 'public task' around the awarding body accreditation and any government funding activity. An example of this would be where an individual undertaking requests the right to have their data erased but are currently enrolled as a learner.

Requesting access, amendment, erasure and limiting processing of personal data: such as a 'Freedom of Information' request

Any individual may make a request for accessing, amending, erasure and the limiting processing of personal data. If a learner or employer wished to make such a request, they need to;

- Contact Envisage making it clear the individual right they are exercising in writing

  Envisage contact details:

  The English Institute of Sport
  Coleridge Road
  Sheffield
  S9 5DA
  Telephone: 0114 223 5675
  E-mail : info@envisagetraining.co.uk

Or contact the Envisage's Data Protection Officer (DPO) directly, if the response from Envisage to written/email request is unsatisfactory or untimely (>10 working days).

Envisage's Data Protection Officer (DPO) contact details:

David Ireson
The English Institute of Sport
Coleridge Road
Sheffield
S9 5DA
Telephone: 0114 223 5675
Mobile: 07899973650
E-mail : david@envisagetraining.co.uk

Upon Envisage receiving a written/email request from a learner or an employer's in relation to data rights of their identified personal data that is held by Envisage, Envisage will:

- Refer the employer or learner's request to Envisage's DPO (Envisage's Owner) to immediately review of the data request
- Ensure the data request is actioned and a response is issued to the learner or employer within 10 working days.

Children (under 18) Personal Data

The Information Commissioner's Office (ICO) definition of a 'child' as anyone under the age of 18 (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/), Envisage will work within ICO and GDPR requirements with regard to the processing, retention and erasure of children's personal data.

Along with ICO and GDPR legal guidelines for children's data processing, when working with 16-18 year olds, Envisage will;

- deliver education and training to learners aged 16-18 (with no additional needs and/or EHCP identified or disclosed), Envisage require consent of the learner through a permission to share data document, signed by the learner, prior to processing personal data.

A 16-18 year old child has the same 'individual rights' relating to personal data stored by Envisage as other adult learner or employer. For a 16-18 'looked after child' or a 16-18 child in local authority care, Envisage will liaise with local authority agencies and the child's guardians to ensure the child's needs and interests are safeguarded and fully supported in their education and training course decision and subsequent data sharing.

The level of consent required for a 16-18 child with regard to personal data collection will be based upon an assessment 'competency' at the time of their interview for an education and training qualification with Envisage.

Where Envisage may have issues or concerns of the learner's ability and/or their learning ambition/commitment, Envisage would encourage the learner to discuss their ambitions with their carers or parents. Envisage would also seek the learner's permission to work with their parent(s)/carer(s) to support the 16-18 learner's learning journey/decisions. They would still be able to exercise their individual rights in the same way as an adult learner or an employer.

Data security

Envisage will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. To ensure data security;

- Access to our databases is restricted through password protection. Only team members nominated by the Envisage partners have access to the system
- Envisage computers and other data storage devices are secured to protect against theft of machinery and thus loss of data. Files that hold confidential information of any kind are kept secure (personal information is always considered confidential)
- Paper documents that are not required for archiving are shredded. Any portable storage devices that contain personal information are physically destroyed when they are no longer required.
- Envisage team members will ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- All Envisage computers will be protected by up to date virus protection
- Envisage will ensure that all of its team members receive GDPR CPD training and updating on their specific responsibilities around GDPR and Envisage's Information Security guidelines. All Envisage staff and associates will adhere to the GDPR legislation, Information Security guidelines and current good practice

Data Security Breaches

Envisage has an organisational process in place to deal to any potential data breach. The ICO define a data breach as a;

'Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.'

Personal data breaches may include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending staff and/or learner personal data to an authorised or incorrect recipient
- the loss of any digital/computing device that can lead to staff and/or learner personal data being lost or stolen
- the unauthorised alteration of staff and/or learner personal data without the permission of the staff or learner and Envisage management/DPO
- any loss of availability of personal data through accidental erasure of personal data, including hard copy and/or digital copies

Envisage Data Breach Process Flowchart

Envisage will in the event of an identified data breach of personal data use the following flowchart to mitigate and manage breach of personal data:

1. Recording & Monitoring of a data breach

The organisation commits to record any potential or actual breach of data on a data breach register.

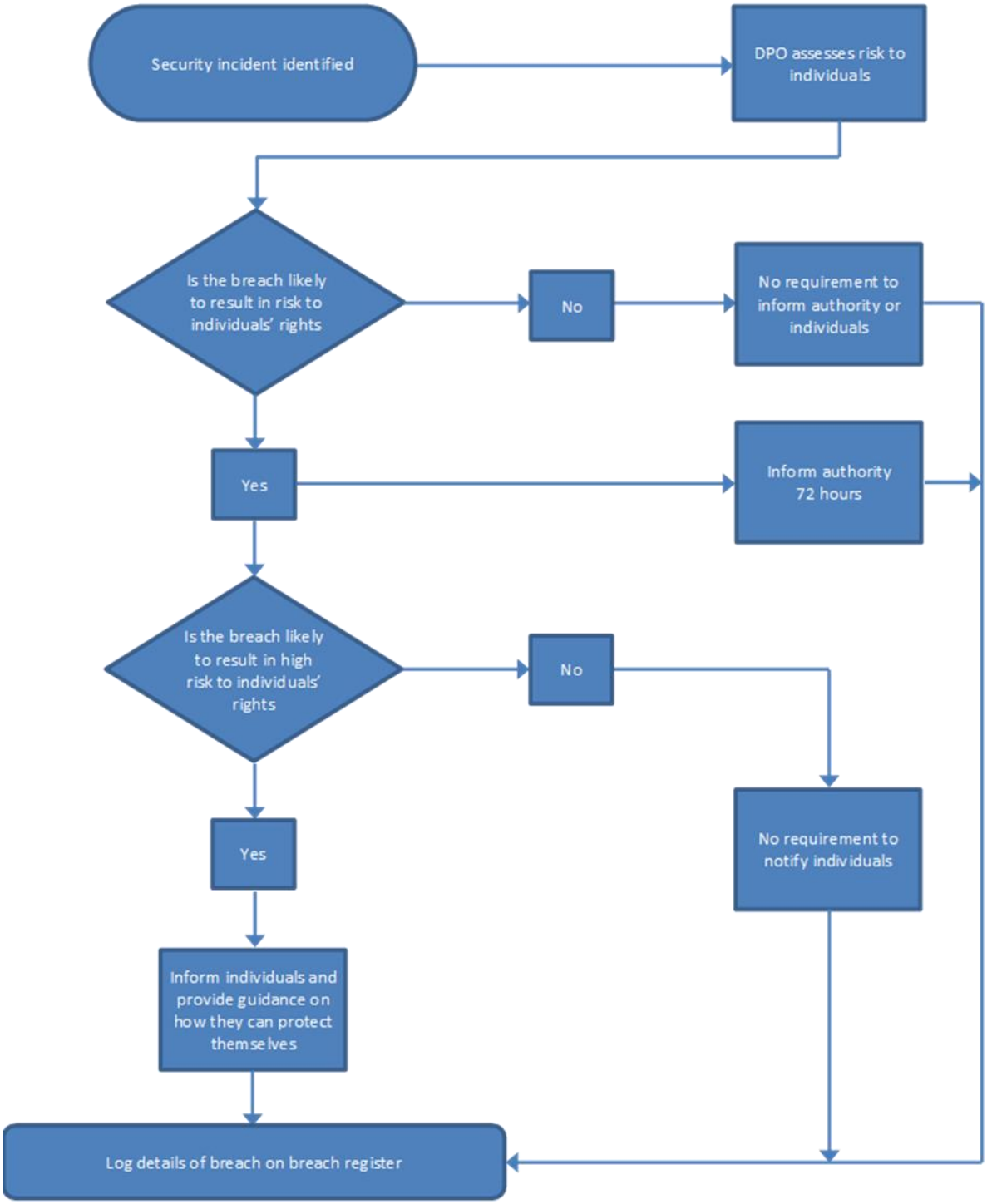
In the event of an identified potential or actual data breach the organisation commits to:

- Report the data breach immediately to the Data Protection Officer (DPO)
- Record on a Data Breach Register (See Appendices 4.1 for example) any incident which potentially or actually leads to a breach of data.
- Document via Data Breach Report (See Appendices 4.2 for example) the full details of the data breach and actions undertaken in accordance with GDPR requirements.
- Notify the affected individual(s) affected by the data breach where appropriate.
- Notify the ICO of any actual data breach within 72 Hours.

The Envisage Owner/Data Protection Officer, will manage and monitor the process involving any data breach, including notification to the ICO within 72 hours. If the Owner/DPO is unavailable the Envisage Compliance and Contract Manager will assume responsibility for managing, completing and reporting the data breach through the decisions and actions within the Envisage Data Breach process.

1. Envisage Data Breach Process Flowchart

Envisage will in the event of an identified data breach of personal data use the following flowchart to mitigate and manage breach of personal data:



Data Security Breach – Register (example)

Envisage Data Security Breach Register				
Incident number	**Type of breach**	**Logged by**	**Date**	**Comment**
001	Learner personal details emailed to unauthorised person	DI	01/10/20	Report filed.
002	Loss of staff laptop	IP	11/10/20	AS has lost his work laptop on 10/10/20. Unable to locate it at home or work

Data Security Breach – Report (example)

Envisage Data Breach Report	
Breach number: 002 Date completed: 11/10/20 Reported to: D Ireson DPO	Breach register completed by: I Philip Date reported: 19/10/20
Details of the breach and type of data	AS has been unable to find his Envisage laptop at work or at home.
How has this been identified	Last used his laptop in Envisage office on 10/11/20 evening and remembers taking it home
Who has been affected	Laptop has no learner data & is encrypted/password protected
Have the affected persons been notified	Not applicable
Consequences of breach	• No risk of learner/staff personal data being accessed • There is low risk of the laptop being accessed by any unauthorised person(s)
Remedial Action	Envisage staff reminded to update security of laptops, check/ensuring no storage of learner or personal data on laptops & updating laptop password protection
Does ICO need informing of breach	No
Does Envisage risk register require updating	No
Comment	Low data breach risk, isolated incident, staff awareness planned with no further action required. Laptop was found 4 days later – 15/10/20
Signature: D Ireson	

Document Name: Envisage GDPR Policy		Authorised by: Dave Ireson
Version: 2	Version date: 07/06/2023	Version next review due : 07/06/2024