Introduction

This document is intended to be a short summary of the General Data Protection Regulations (GDPR) and how they *may* potentially be applied in the context of educational providers who offer Access to HE Diploma titles (or other regulated qualifications) in relation to quality assurance.

Nothing contained herein constitutes '*legal advice*'. The document makes no claim to be a definitive statement of what constitutes compliance and reference should always be made to the ICO guidance as well as the provisions of the GDPR and the *Data Protection Act (2018)* in framing any centre level **Data Protection Impact (Risk) Assessment**.

Practitioners should also seek guidance from their centre's **Data Protection Officer** in relation to any matters arising where applicable.

This document also does not reference what should occur where a breach is identified. Reference should be made the ICO guidance where any such breach occurs. [1]

The document simply sets out the provisions of the legislation and identifies procedural/protocol issues which may generally arise for Access providers, together with potential responses which may (or may not) be appropriate in resolving said concerns. It also presents possible mechanisms to improve security and address areas of potential non-compliance in relation to External Quality Assurance.

In managing any issues emerging from GDPR, the primary source for guidance must remain the legislative provisions themselves and the relevant guidance from the Information Commissioners Office.

Useful Sources referred to in developing guidance:

ICO Guidance on Lawful Basis for Processing Data:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

ICO Guidance on Special Category Data
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

ICO Guidance on Security:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

[1] For further guidance see: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

General Principles

At its heart, the GDPR is based upon a general requirement that data must be handled securely such that any data processing is *generally lawful, fair and transparent*.

Any data held/processed must be held securely and any processing should conform to the 'CIA Triad'. This means all systems processing of data must uphold the three principles of Confidentiality, Integrity, and Accessibility.

The regulations make a clear distinction between personal data which must still be held and processed securely and special category data/criminal offence data, which are both judged to be higher order information which demands additional safeguarding.

What is special category data?

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Source: ICO (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/)

Data in relation to criminal convictions is subject to similar, but separate safeguards to ensure that it is held confidentially.

As previously noted, where special category data is processed there needs to be additional safeguards in place. There must be a clear statement which identifies a lawful basis for holding data associated together with an identifiable secure system of processing and a **Data Impact Risk Assessment** which sets out the system. Where any data held by a provider relates to any of the above (whether this is centrally held data or individual departmental/individual tutor data), then due reference must be made to the provisions of the legislation.

For many centres there will be central systems which provide a secure basis for holding and processing data (together with an established/identified **Data Protection Officer**). However, for example, where an individual tutor may keep records of a student's progress and note within them health issues or any narrative which may be covered by the regulations (outside of the central system), this data would still be covered, and any systems would need to be demonstrably compliant with the GDPR and Data Protection Act (2018) provisions. Tutors should be mindful of this in terms of any parallel recording systems used (whether paper based or electronic).

Lawful basis for Retaining/Processing Student Information

In all cases, the first thing which must be established is a lawful reason for processing data. The legislation suggests processing must be necessary and proportionate to achieve specific tasks. Necessary does not mean essential, but it does require that there is good reason, and any objective of processing could not be achieved by other means.

These provisions apply to all data held (not only special category data or criminal convictions). Article Six of the GDPR establishes six potential lawful bases for holding and processing data:

GDPR: Article Six (lawful basis for processing data):

a) Consent
b) Contract
c) Legal Obligation
d) Vital Interest
e) Public Task
f) Legitimate Interest

Further information can be found at: https://www.legislation.gov.uk/eur/2016/679/article/6

Learning agreements with students may well include specific provisions relating to Consent (a) for data processing which allow for student consent. However, it is important to ensure that this is the case, and it should be remembered that consent has within it the right of withdrawal.

Contract (b) may also be evoked in relation to the sharing of student work in the sense that the centre will have a contract with the student for the provision of a specified qualification (Access) and to fulfil the potential for the award of the qualification the work must be shared for verification purposes. Therefore, it would not be in the individual student's interests for the work not to be shared. This argument does not necessarily extend to any information which might constitute special category data.

Public Institutions such as colleges and universities will likely refer to Public Task (e) in that as designated public authorities most will satisfy the criteria set out in the *Freedom of Information Act (2001)*[2]. In this instance, there will be a clear public good rationale for the proportionate and necessary lawful processing of data. However, Legitimate Interest (f) may also be referred to as a basis for data processing where it is necessary for the institution, or a third party (Access Validating Agency (AVA)) to hold and process data in

[2] See: https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/freedom-of-information-and-environmental-information-regulations/public-authorities-under-foia/ for further guidance

relation to the public good (e.g. the award of a qualification to the student). However, the notion of Legitimate Interest (f) is limited where there is good reason to protect personal data.

The above is not intended to constitute legal advice to practitioners. However, it aims to establish the need for any data processing to be undertaken only based on the requirements of the legislation.

Therefore, a clear and appropriate rationale for processing data must be established which is proportionate and necessary.

Sharing information with LASER:

As an AVA, LASER is required to hold and process data on registered students. This is necessary for both the accreditation of individual students and for the demographic monitoring requirements placed on Access providers by the QAA (and ultimately the government). Indeed, all centre agreements state that centres will comply with AVA requirements in terms of (inter alia) moderation and monitoring establishing a clear third-party imperative for the sharing of necessary data.

If this information is not shared, then accreditation cannot take place meaning the individual student cannot progress. However, data must be shared securely and in terms of special category data, the student has a right to withhold information (for example gender, ethnicity, or ability). This information can only be shared with student consent (see below).

Learning agreements should make it clear that information will be shared with the relevant AVA and the student's right not to share certain information should be made clear.

Special Category Data

Where data constitutes special category data, this requires a further legal justification as set out within Article Nine of the GDPR.

GDPR Article Nine: Special Category Data (Lawful Basis for Processing).

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

See: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

A centre would likely refer to 9(g) in relation to *Reasons of Substantial Public Interest* as a basis for processing special category data.

This requires reference to be made to the 23 conditions set out in paragraphs 6 to 28 of Schedule One of the *Data Protection Act (2018)* for establishing public interest.

Schedule One of the Data Protection Act (2018).

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

It is likely that centres would refer to (8) in lawfully holding certain categories of significant personal data in meeting the requirements for demographic monitoring. However, in this instance protocols should allow the student to withhold data in this respect (which is their right).

Sharing special category demographic data with LASER:

The QAA and ESFA require demographic information as a part of their reporting. As noted, this information allows LASER to monitor achievement and grading and to further understand the impact of certain demographic factors on student progression. The above provides the lawful basis for facilitating this analysis.

Whilst a student does have a legal right to withhold data, centres should encourage this data to be shared as it has a significant value in understanding the factors which impact upon both achievement and grading and how provision may be improved.

In certain instances, there may be potential reference to (16) and/or (17) where information is held in relation to additional support/counselling[3] to directly support the student (once again this is subject to the right of the student to withhold said information).

Extenuation and mitigation applications:

In instances where a student is applying for extension, extenuation, mitigation, or reasonable adjustments there is an inevitable requirement for data sharing with the External Quality Assurer. In these instances, QAA Regulations require that any award board decisions in relation to the above are formally agreed by both the External Quality Assurer and the AVA. This creates a situation where special category data pertaining to health and well-being will almost inevitably be shared.

*It is the view of LASER that any specific evidence (e.g. medical evidence) should **only** be shared with the relevant External Quality Assurer in relation to the above. The award board only needs to confirm that due process has been followed and that the External Quality Assurer supports whatever measures are to be taken. Information sharing should be as limited as is possible in relation to the individual circumstances and where information is shared electronically this should be encrypted and where possible anonymised (see Data Security below).*

In terms of **Criminal Offence Data** there must also be a lawful basis for the holding of such data. This can again be demonstrated through reference to the Data Protection Act (2018) Schedule 1(17) as necessary in relation to counselling provision.

Data Security

All data held must be processed in line with the provisions outlined in Article 5(1f) of the GDPR which states all data must be:

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…

All data held must be handled and processed securely in line with the CIA triad (previously mentioned). Systems must clearly protect confidential information (especially but not limited to special category data and any information on criminal convictions).

Whilst the GDPR and the ICO do not establish clear statements of how this may be achieved, they do recommend pseudonymisation and encryption as potential tools to hold and process data effectively where the information is held electronically. However, paper-based information is equally liable to being held securely, with reference made to appropriate levels of physical security such that information remains demonstrably secure and confidential.

[3] Where centres offer counselling provision to support students the data handling processes employed by College Counsellors will also be subject to regulation (although as noted, the Data Protection Act (2018) does provide appropriate support for holding data in relation to Article 9(2g) of the GDPR subject to lawful and secure data processing.

Anonymisation occurs when any identifiable references to the identity of the data is removed and cannot be re-established. This may well be helpful in terms of the sharing of data sets where the data will not require any identification of the student. However, it is often necessary for AVAs to sample work or access information in relation to such matters as extenuation and mitigation which needs to be accessed with specific reference to the individual.

In this instance, pseudonymisation may be used whereby the identity of the student(s) is/are removed and replaced with a code within the shared documentation. The document is also securely encrypted via a separately shared password. Any identification is effectively removed. The code(s) to translate the information back in relation to the student(s) would then be shared separately via an encrypted key(s) to maximise security.

A key requirement here is that all data transferred should be undertaken using a secure system such as the LASER SharePoint or secure alternative (by agreement), to maximise security.

All LASER External Quality Assurers are contractually bound by the provisions of data protection legislation and will process data securely as a matter of course in line with overall LASER policy.[4]
It is worth remembering that e-mails are not secure and USB/Flash Drives are equally insecure (unless they are encrypted, even then they are less secure due to their potential for loss).

Whilst matters relating to extenuation/mitigation are exceedingly likely to relate to special category data in relation to health, it is equally worth remembering that even student assessments may contain reflective commentary or identification of health issues which may lead them to constitute special category data. It could be argued that assessed work may reveal political opinions or beliefs in framing arguments. Therefore, processes should ensure that samples are systematically held and processed securely as a matter of course. This does not only relate to electronic data, but also to hard copies of relevant information. Any internal retention of samples of student work for internal standardisation should also conform to the requirements of the GDPR even if they are not shared externally. The LASER publication: 'Addenda to the Quality Assurance Handbook' sets out the requirements for retention of sampling for internal standardization purposes and also the data protection implications.

Therefore, where information is being shared (especially relating to special category data), due diligence should be undertaken in line with relevant policy. The use of the LASER SharePoint platform for all data sharing is strongly encouraged as this presents a secure platform for all Access related data sharing. Any alternative employed should be secure and should also facilitate effective data sharing in line with the provisions of the regulations.

[4] LASER-Privacy-Notice.pdf (laser-awards.org.uk)

A Final Thought

Please also remember that in identifying and holding/processing any data, the provisions of the legislation apply not only to students but also employees/colleagues or indeed other relevant third parties (e.g. participants in research studies[5] or information about others contained in reflective logs). It is vitally important to remember that any personal data must be held securely as a matter of course (especially special category data and criminal convictions). Where relevant, data should be anonymised, pseudonymised and/or encrypted depending on context. This should be seen as a general principle that applies without exception. The systems noted above in terms of holding information securely apply in relation to any personal data held, not simply relating to students but also to others within any institution.

As previously stated, **this document does not constitute legal advice**, but rather attempts to provide some guidance about the potential issues arising from GDPR and some mechanisms for recognising when (and why) data sharing is necessary and why/how it must be achieved securely. The individual circumstances of different centre/providers and their internal systems mean that the guidance contained here may (or may not) be appropriate in framing practice. However, all centre/providers must ensure that data is held securely and safely regardless of their approach and any systems and protocols must demonstrably adhere to the requirements of data protection legislation.

Guidance Approval

Approved internally by CEO, 11 January 2024
Approved externally by AQDC, 11 March 2024
Latest review date: March 2029

Please note:
This guidance is specifically relating to delivery of Access to HE qualifications.

[5] Centres should ensure that any IAS work completed respects the provisions of the GDPR as a matter of course. However, it is worth restating that this is both a legal imperative as well as an ethical one.

Addenda to Laser Learning Awards (LASER) Document: Guidance for Practitioners on Potential Implications of Data Handling

Artificial Intelligence (AI) and data sharing

The increasingly fast paced development of Artificial Intelligence (AI) platforms presents many potential opportunities and advantages for those working within education. It also forms a significant challenge for educators in relation to ensuring the validity of student assessments. Current discussion of AI has tended to focus on its potential legitimate and illegitimate use by students as an aid to study or conversely a mechanism to cheat (plagiarism by AI). These factors have been discussed in some detail the following LASER documents / On-Line provision:

- LASER Guidance on Use of Artificial Intelligence: Guidance_on_Use_of_AI.pdf
- LASER Course on AI: https://www.laserconnect.org.uk/courses/an-introduction-to-ai-in-education/

AI also presents a tool which teachers and educators may use to develop teaching resources (for example power-points), to provide feedback on student work (subject to checking) and to run analysis of data. For example, it is possible to upload a spreadsheet into platforms such as 'Co-Pilot' or 'Chat GPT' and to then request it to run data analysis on the material contained within the data set.

It is vital that practitioners are mindful of the provisions of any Privacy Agreements / Policies in relation to the AI tools they employ prior to their use to ensure that any data uploaded, and materials shared or created using AI technologies does not lead to a breach the provisions of the GDPR. For the avoidance of doubt, where material is uploaded to AI platforms, in many cases this will be retained and potentially used by said AI platforms for purposes beyond that of the upload. Therefore, any upload of student work or data inevitably results in said material being shared with a third party (the AI platform itself).

Therefore, it is of the utmost importance that privacy and data sharing provisions for the platform are checked to ensure that any data sharing will remain compliant with the provisions of the GDPR. Any use should be subject to consideration within the relevant **Data Protection Impact (Risk) Assessment.** There will also be a need for a lawful basis for said data processing.

This is not to say that AI cannot be used by practitioners for marking or data analysis, it simply affirms the need for security and privacy to be considered as a key aspect of the decision-making process. Whilst AI may bring many time saving benefits in terms of planning materials, providing resources, and running analyses, this must not carry with it the unintended consequence that personal data of any kind enters the public domain. There are equally ethical concerns in relation to AI led decision-making and explainability which must be considered which practitioners should also consider in deciding what constitutes the appropriate use of the technology.

Useful Links to Resources:

ICO: Guidance on AI and Data Protection
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

ICO: Accountability and Governance Implications of AI
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/#DPIA

JISC: Artificial Intelligence and Ethics – GDPR and Beyond
https://regulatorydevelopments.jiscinvolve.org/wp/2020/04/22/ai-and-ethics-gdpr-and-beyond/

EU Guidance: The Impact of GDPR on Artificial Intelligence (Report)
https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Updated: 11 March 2024