

# Data Protection and Privacy Policy

## Contents

Overview .....	3
Data (Use and Access) Bill Overview .....	3
Policy Scope .....	3
Who is this policy for? .....	4
Purpose.....	4
Principal Data Sharing Stakeholders .....	4
Definitions .....	4
Personal data and special categories of personal data.....	6
What Personal Data does PAL Process? .....	7
Why we Process Personal Data and our Legal Basis for Processing .....	8
Lawful Consent for Processing Data.....	9
How do we collect your personal data? .....	10
Data Protection Principles and how we process your Personal Data .....	10
Data Protection .....	12
Data Protection Officer.....	12
PAL Board.....	12
Training.....	13
Roles and Functions.....	13
Data Protection by Design & Default .....	14
Sharing your Personal Data .....	14
Provider, Employer and Apprentices Responsibilities' (clients/customers) .....	15
Your Rights- Access to your Personal Data.....	16
Subject Access Request (SAR) .....	16
Children & Subject Access Requests.....	17
Responding To Subject Access Requests .....	17
Manifestly Unfounded and Excessive .....	18
Responding to Requests that involve others (third parties) .....	18
Assessment Marks and Grades .....	19
Assessment scripts, recordings, and Assessment marks .....	20

Security and Data Security Breach Management .....	20
Personal Data Breaches.....	20
When does PAL need to tell Individuals about a Breach? .....	21
Data Security.....	22
Data Retention.....	22
Complaints and Enquiries Regarding Data Processing- How to Contact PAL .....	23
Contacting the regulator .....	23
Monitoring and Review .....	23
Regulatory references .....	23
Appendix One-Personal Data.....	24
Appendix Two -What Information we process and why .....	27
Appendix Three- Subject Consent .....	30
Appendix Four Privacy notice digital assessment recordings webinars/events/ pre-recorded pieces to Camera 31	
Appendix Five Data (Use and Access) Bill Overview .....	35

## Overview

All our stakeholders should feel confident in Professional Assessment Limited (PAL's) handling of their personal data and how we use such data and be assured that we will only request and process essential data and that we strive to ensure data and information is collected, recorded, and compiled accurately and only used for stated purposes.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

PAL is committed to a policy of protecting the rights and privacy of individuals, staff, associates, consultants/TAs, and others in accordance with Data Protection Legislation<sup>1</sup>. This policy applies to all personal data processed by PAL.

This Policy explains in detail how we collect personal data, the reasons for this collection, the legal basis for processing and how we handle and maintain the security of the personal data we process.

To note we may change this privacy policy without notice. Please check back frequently to see any updates or changes made to this statement.

This Data Protection and Privacy Policy is for Professional Assessment Ltd. **Our ICO registration number is ZA275792.**

## Data (Use and Access) Bill Overview

The Data (Use and Access) Bill aims to enhance data access and usage across various sectors to boost the UK economy, improve public services, and simplify citizens' lives. Introduced in the House of Lords on 23 October 2024, it has progressed through various stages and is set for its second reading in the House of Commons on 12 February 2025. This policy will be reviewed and updated when the bill becomes law. Please see appendix five for a summary of the proposed Data Use and Access Bill.

## Policy Scope

The policy covers data processing relating to:

- PAL staff
- PAL Associates and Consultants/TAs
- Individuals external to PAL – for example, an apprentice or learner, when a person applies for a role at PAL, when an organisation provides PAL with data or services to support our data collection and processing activities for our core work

This policy relates to apprenticeship assessment activities, PAL will review this policy in the light of future changes to assessment activities as stipulated in the assessment principles of 2025. For qualification activities please refer to the AO policy.

The company holds and processes information about company employees, associates, apprentices, and other data subjects for academic, administrative, and commercial purposes.

PAL's service level contracts, along with our EPA<sup>2</sup> manual, refers to PAL's approach regarding data management and protection and should be read in conjunction with this policy.

---

<sup>1 1</sup> From 1<sup>st</sup> January 2021, the law relating to data processing in the UK changed. Any processing of data prior to 1<sup>st</sup> January 2021 has been undertaken in accordance with EU General Data Protection Regulation (EU) 2016/679 ("the EU GDPR"). From 1<sup>st</sup> January 2021, the EU GDPR no longer applies to the UK. The UK has retained the EU GDPR under Section 3 of the European Union (Withdrawal) Act 2018 (EUWA). It has been renamed as the UK GDPR and tailored by the Data Protection Act 2018. From 1<sup>st</sup> January 2021, the UK data protection regime consists of the UK GDPR as incorporated under the EUWA and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC) and the Data protection Act 2018 as enacted in May 2018 and amended by the DPPEC Regulations.

<sup>2</sup> Please note EPA is a term applied to current assessment practices and assessment plans, as new assessment plans are introduced, and terminology changes PAL will update this policy

It includes information held on computers (including email), paper files, photographs, audio and video recordings and images.

### Who is this policy for?

This policy is intended for Employers, Providers, Employer Providers Apprentices, Suppliers, PAL personnel and PAL Associates and Consultants/TAs.

Centre and Qualification work is covered by an AO Data Protection and Privacy Policy and whilst much of the information is shared across both policies, the individual policies recognise the context and accountabilities of being an AO and acting as an EPAO.

### Purpose

All personal data must be handled and dealt with appropriately however it is collected, recorded, and used, and whether it is on paper, in electronic records or recorded in other formats, on other media, or by any other means. This policy outlines the context of data protection for PAL and defines roles and responsibilities and highlights the importance of effective data management protocols and procedures

**In conducting our EPA activities, the data we collect and collate from third parties about an individual apprentice serves a legitimate interest, PAL needs the data to perform our assessment activities, to include certification requests.** To support certification requests we ask the apprentice to consent to PAL requesting their certificate, we document this consent at our assessment planning.

For PAL personnel the policy advocates the need for accuracy and security in respect of data collection, collation, and storage. For third parties such as providers, employers and apprentices, the policy aims to demonstrate PAL's approach and high importance we place on data and information management, checking of data with third parties and suppliers to ensure accuracy and how we securely store data.

### Principal Data Sharing Stakeholders

Where PAL is required to share data for certification purposes, PAL provides DfE with the required information that identifies the individual apprentice, the apprenticeship standard, and the outcome. The information is shared via a secure API.

Where PAL is required to share data in the public interest, with the qualification regulators, PAL will provide this data in the required format and share via the appropriate secure portals.

DfE and qualification regulators, in PAL's case the regulator is Ofqual, are obliged to have robust data protection policies and procedures that are fully compliant with UK Data Protection and Privacy legislation.

### Definitions

- Data controller – is a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others as a joint data controller, determines the purposes of any personal data and the means of processing it.
- Data Processor- is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of the data controller.
- Data controller agents- is any person who processes data within the data controller organisation, for PAL these will include any PAL staff member or associate who processes personal data.
- Data Protection Officer – The Data Protection Officer (DPO) assists PAL to monitor internal compliance, inform and advise on our data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner

- “Personnel”,<sup>3</sup> “apprentices” and “other data subjects” may include past, present, and potential members of those groups.
- Data Subject- The identified or identifiable individual whose personal data is held or processed.
- “Other data subjects” and “third parties” may include contractors, suppliers, contacts, referees, and friends.
- “Processing” refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing, or destroying information.
- Personal Data Breach- A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- Agents of the Data Controller- PAL personnel who process personal data under the requirements of PAL’s policies and procedures

PAL, as a data controller, is responsible for, and must be able to demonstrate compliance with these principles. We follow procedures to ensure that all employees, contractors, agents associates, consultants, and other parties who have access to any personal data held by or on behalf of us are fully aware of, and abide by, their duties and responsibilities under data protection legislation.

All PAL staff and commissioned associates and consultants/TAs are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to personal data.

#### **Changes since Brexit**

The EU’s GDPR has been lifted into a new UK-GDPR that took effect on January 31<sup>st</sup>, 2020. An adequacy decision for the UK and the Law Enforcement Directive (LED) was adopted on June 28, 2021, by the EU, securing unrestricted flows of personal data between the two blocs until June 2025.

The DPA 2018 continues to set out the framework for data protection law in the UK. It was amended on 01/2021 by regulations under the European Union Withdrawal Act to reflect UK’s status outside of the EU.

#### **The main changes to the old regulations are:**

- **Transparency- more detailed and informative privacy notices are required**
- **The purpose of, and legal basis for processing data must be explained in clear and simple terms**

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the way you interact with European data protection authorities has changed.

The EU Commission must monitor developments in the UK on an ongoing basis to ensure that the UK continues to provide an equivalent level of data protection. The Commission can amend, suspend, or repeal the decisions if issues

---

<sup>3</sup> Personnel includes PAL employees, associates and consultants/TAs and advisory group members

cannot be resolved. Also, EU data subjects or an EU data protection authority can initiate a legal challenge to the decisions. The Court of Justice of the European Union would then have to decide whether the UK did provide essentially equivalent protection.

All PAL personnel are aware of the requirements of the UK GDPR. They appreciate the impact of this piece of legislation and the associated updates and of areas of work that could cause potential compliance problems under the GDPR. The Business Operations Director and Director of Audit and Compliance will be responsible for staff training and compliance.

We are committed to ensuring that the principles of data protection that predicate GDPR are embedded into everything we do.

PAL notes that the DUA readings have highlighted the challenge of adequacy with EU GDPR and will amend policy and procedures in light of the DUA act, whilst maintaining practices that are contingent with universal perceived good practice.

### **Personal data and special categories of personal data**

This policy applies to personal data as defined by the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR)<sup>4</sup>; that is, any information relating to an identified or identifiable living person. It will cover information which on its own does not identify someone, but which would identify them if put together with other information.

The UK GDPR extends the definition of personal data to include identification numbers, such as Unique Learner Identifier Numbers (ULIN). Personal data may include an individual's IP address and social media name.

#### **See Appendix One- for further information regarding personal data**

This policy also applies to **special categories of personal data**<sup>5</sup>. Special category personal data is data that is particularly sensitive and therefore merits specific protection. The special categories of personal data specifically include data relating to an individual's:

- racial or ethnic group political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data and/or biometric data health
- sexual orientation

#### **What are the conditions for processing?**

- (a) Explicit consent.
- (b) Employment, social security, and social protection law.
- (c) Vital interests.
- (d) Not-for-profit bodies.
- (e) Made public by the data subject.
- (f) Legal claims and judicial acts.
- (g) Substantial public interest.
- (h) Health or social care

This policy also applies to criminal offence data<sup>6</sup> to the highly limited extent such data is processed by PAL.

---

<sup>4</sup> Article 4 of the UK GDPR

<sup>5</sup> As defined by Article 9(1) of the UK GDPR

<sup>6</sup> Article 10 of the UK GDPR

Further information is available in PAL's appropriate policy for handling sensitive information, and PAL's recruitment policy for people with criminal convictions available on request from PAL's DPO.

All personal data within PAL's control shall be identified as personal data, special category personal data or criminal offence data to ensure that it is handled in compliance with legal requirements and processing does not breach the rights of the individuals to whom it relates.

## What Personal Data does PAL Process?

**For the purposes of data protection legislation, PAL is a data controller.** PAL is required to manage data protection to meet the standards of DfE, the qualifications regulatory body, the ICO and other relevant agencies.

PAL collects personal data from a variety of sources. This can range from personal data given to us directly when you contact us, personal data we receive to facilitate end-point assessment to personal data used for HR purposes.

We process personal data relating to:

- Employees, including job applicants
- Associates
- Consultants/TAs
- Suppliers and service providers and Training Providers
- Apprentices (i.e., individuals registered to undertake EPA)
- Employers (i.e., employer representatives who are named as the individual supporting the apprentice at work)
- Providers (individuals who represent the Provider and are PAL's main point of contact with main provider)
- Individuals who make enquiries, complainants, and their representatives (including whistle-blowers)
- Respondents and their responses to consultations and surveys and feedback questionnaires
- Event or webinar attendees
- Other stakeholders (such as individuals in government departments and regulatory agencies)

Examples of Personal Data PAL may process	Examples of Special Category Data PAL may process
<ul style="list-style-type: none"><li>➤ Names of individuals</li><li>➤ DOB (apprentices/learners)</li><li>➤ Unique Learner ID (ULIN apprentices/learners)</li><li>➤ UKPRN- Provider identifier</li><li>➤ Proof of ID documents</li><li>➤ Assessment grades and outcomes</li><li>➤ Contact information (for example postal address, telephone number, email address- range of stakeholders to include PAL personnel)</li><li>➤ Information in relation to activities, to include enquiries and appeals; complaints; maladministration and malpractice; conflicts of interest and sanctions</li><li>➤ Information from consultations and feedback</li><li>➤ occupation or job title places of work</li><li>➤ Information about an individual's education and qualifications information about an individual's skills and expertise, for the purpose of recruitment, engagement and assessment allocations and assignments</li><li>➤ Previous attainment and achievements of qualifications where evidence of attainment is necessary entry requirement prior to assessment or recruitment</li><li>➤ Other information relevant to our HR function</li></ul>	<ul style="list-style-type: none"><li>➤ Physical or health details</li><li>➤ racial or ethnic origin</li><li>➤ Religious or other beliefs</li><li>➤ Political opinions</li><li>➤ Sexual life</li><li>➤ Trade union membership</li></ul>

Examples of Personal Data PAL may process	Examples of Special Category Data PAL may process
<ul style="list-style-type: none"> <li>➤ Photographs, visual images, and recordings where presented as contributory evidence for apprenticeship assessment and demonstration of competence</li> <li>➤ Data such as DSTATS to support audit and compliance work</li> </ul>	

### Criminal Offence Data

PAL may process personal data relating to the charge or alleged charge of a criminal offence by an individual and relating to legal proceedings, outcomes and sentences or convictions in respect of such offences to the extent that such matters are relevant to PAL's functions. For example, we may process criminal convictions data where it is necessary for us to do so as an employer, or where such data is relevant to the exercise of our role as an EPAO/AO (for example in circumstances where an individual has infringed PAL's intellectual property rights and confidentiality of assessment instruments or where there has been an incident of serious malpractice and fraud).

**See Appendix Two – What Information we process and why**

### Why we Process Personal Data and our Legal Basis for Processing

We process the above information to carry out one or more of the following activities:

- PAL is responsible for making sure that apprenticeship assessments for apprenticeship standards meets the requirements of the relevant regulatory body (Ofqual) and are congruent with the requirements of DfE. Apprenticeship programmes to be eligible for funding must comply with the Apprenticeships, Skills, Children and Learning Act 2009 and apprenticeship programmes should adhere to a specific set of industry ratified occupational standards and associated Apprenticeship assessment plan, approved by Skills England. PAL as an EPAO/AO processes information to support assessment and apprenticeship certification requests.
- For any other awarding organisation 'awarding' function PAL is required to meet regulatory requirements, government funding criteria in relation to the qualification funding and will need where pertinent to comply with the Apprenticeship, Skills, Children and Learning Act 2009
- To comply with contractual obligations, PAL in respect of working with providers and in respect of our commercial audit work, issues contracts which outline terms and conditions for delivering our services
- To undertake effective tendering and commissioning activities, to ensure value for money and appropriate commissioning of services
- To acquire consent to apply for apprenticeship certificates, from the individual apprentice
- To review and process data and information for reasonable adjustments and special considerations
- Consideration and investigation of complaints, enquires and appeals, maladministration, and/or malpractice and the processing of sanctions in the development, delivery or grading and issuing of results of apprenticeship standards
- Collection and evaluation of feedback, research, and consultations to improve our service offering
- Supporting and managing our employees and contractors
- Carrying out administrative functions (for example HR, finance, or procurement) maintain our own records and accounts
- Providing or obtaining professional advice



- Sending you information that we think might be of interest to you, if you have consented (such as if you sign up to receive our newsletters)
- Complying with any legal and regulatory obligations PAL is subject to
- Providing data to organisations such as Ofqual and DfE for the purpose of analytical and statistical research in the public interest

## Lawful Consent for Processing Data

The UK GDPR<sup>7</sup> lists six lawful conditions for processing personal data, and at least one condition must apply for an organisation to be able to collect, collate, process and store data that constitutes personal data.

### Six lawful reasons

1. Consent is given to process data
2. Data collection and processing is necessary to perform and undertake business and forms part of the contract between two parties
3. Legal obligation
4. Protection of life
5. The processing of data meets the requirements for being in the public interest
6. Legitimate interests

In most circumstances, PAL's legal basis for processing the personal data for the listed activities are Articles 6(1)(a), (b) and (f). These are:

6 (1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

6 (1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

6 (1) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### Conditions for processing special category data and criminal offence data

The processing of special categories of personal data is only permitted where special conditions apply. Further conditions apply when processing special categories of personal data. In most circumstances, PAL's legal basis for processing special category personal data is covered by Articles:

**Article 9(2)(b)** – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

Processing under this condition would include the information we process for recording staff sickness absences, staff qualifications and training and information required to access benefits such as health insurance.

**Article 9(2)(f)** – for the establishment, exercise, or defense of legal claims

**Article 9(2)(g)** – processing is necessary for reasons of substantial public interest...which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interest of the data subject. In respect of this condition, PAL would process data for statutory and government purposes; to ensure equality of opportunity or treatment; regulatory

<sup>7</sup> See Article 6 of the UK GDPR

requirements and support for individuals with a particular disability or medical condition and safeguarding of children and individuals at risk.

PAL is a regulated end-point assessment organisation, delivering end-point assessment for a range of apprenticeship standards, working with many apprentices, employers, and providers. PAL also offers a commercial and independent audit and compliance function.

As an EPA we are subject to regulation by the qualifications regulator Ofqual, we are also bound by the terms and conditions of the APAR (register), overseen by the ESFA and must comply with the apprentice standards and accompanying assessment plans as published by IfATE.

Examples of data we may process under this condition, include the application and approval of reasonable adjustments in assessments and in specific cases, depending on the circumstances this may extend to the processing of special considerations applications.

Additionally in addressing any disclosures regarding an individual's well-being and safety, from either PAL personnel or others, this condition would be applied in any processing of data and sharing of information with relevant authorities and bodies. Our processing of data in this context is for the purpose of substantial public interest and necessary for the carrying out of our role.

**Article 9(2)(a)** – the data subject has given explicit consent to the processing of those personal data.

Circumstances in which PAL might rely on consent include where we process information about dietary requirements for an event or conference, or where we request or are provided with information to enable us to make reasonable adjustments for individuals regarding how they receive our materials or access our services.

For EPA work we are obliged to seek the consent of the individual apprentice to request an apprenticeship certificate, we request this consent during the assessment planning meeting, and we ask the apprentice to opt in and their decision is recorded on the assessment planning document.

**Article 9(2)(c)** – processing is necessary to protect the vital interests of the data subject or of another natural person. This would include circumstances where we might disclose medical information about an employee in an emergency.

**See Appendix Three- for further information on subject consent.**

**See PAL's Appropriate Policy for Processing Sensitive Information**

## How do we collect your personal data?

Points of collection include:

- Apprentices and Employers contacting us directly and providing information via epaPRO, the platform PAL uses to plan, schedule and co-ordinate assessments
- Our website(s) contact us form
- Various job vacancy and websites/platforms enquiries forms
- Industry events we attend
- PAL personnel or designated agencies commissioned or utilised by PAL as part of our legitimate interests for business development
- Other training, assessment or funding organisations passing us Apprentice or Employer personal data upon legitimate requests from interested and relevant stakeholders

## Data Protection Principles and how we process your Personal Data

The UK GDPR sets out seven key principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy

- 5. Storage limitation
- 6. Integrity and confidentiality (security)
- 7. Accountability

**Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.**

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 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 shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”**

**PAL has a duty to guarantee to data subjects and stakeholders that our data processing is undertaken on a lawful basis and that we are also compliant with other laws such as copyright, industry specific regulations that effect GDPR.**

**Data subjects must also be assured that our collection and collation of data and information is what they could reasonably expect and that we are clear, open, and honest with ‘who we are as an organisation and the nature of our business; why we need specific information, how we will collect and store information; who we share the data with and for what purpose.**

## Data Protection

Some of the ways in which PAL protects personal data include:

### Setting out responsibilities and accountabilities

PAL includes in all job roles descriptions and within our service level agreements with associates and consultants/TAs and service level contracts with third parties (training providers and employers) the requirements and expectations of safe and responsible data processing in line with the UK GDPR regulations and the Data Protection Act 2018.

PAL also has identified, designated person who is a PAL Board member to act as PAL's Data Protection Officer. This policy applies to all staff employed by PAL, and to external organisations or individuals working on our behalf.

Staff who do not comply with this policy may face disciplinary action. Associates and consultants/TAs who do not comply with this policy will be in serious breach of their service level agreements, as well as this policy and such agreements will be subject to termination on PAL Board approval.

Suppliers and third parties are required to comply with the legislation and regulations, this policy is based on, failure to do so may result in termination of arrangements and or sanctions.

### Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. As part of their reporting function, they will report to the PAL Board of Directors, the governing body of PAL.

The DPO is tasked with monitoring compliance with the UK GDPR and other data protection laws, our data protection and GDPR policies, awareness raising and training and self-evaluation (audits) as well as recording and reporting any data breaches. The DPO also acts as the point of contact for the ICO and will support the MD in any communications with the ICO and other regulatory communications.

PAL's DPO is the Director of Audit and Compliance. The DPO can be contacted by individuals whose data PAL processes.

### PAL Board

The PAL Board of Directors are responsible for implementing good data protection practices and procedures within PAL in compliance with the Data Protection Principles. The Business Operations Director on behalf of the Board is responsible for the day-to-day management and operations of data processing and data storage and IT and associated security systems associated for apprenticeship assessment. The Qualifications Director in conjunction with the Business Operations Director, will oversee the day-to-day management and operations of data storage and IT and associated security systems for qualification delivery.

### PAL Personnel Responsibilities

All personnel shall:

- Ensure that all personal information which they provide to the company in connection with their employment is accurate and up to date
- Inform the company of any changes to information, for example, changes of address
- Inform the company of any errors or, where appropriate, follow procedures for up-dating information
- Respond to information requests, such as a DVLA check in a timely manner

**The company will not be held responsible for errors of which it has not been informed.**

When personnel acting as data agents hold or process information about apprentices, employers, providers, colleagues, or other data subjects (for example, apprentices' assessment evidence such as projects, references, or details of personal circumstances), they should comply with the following:

Personnel shall ensure that:

- All personal information is kept securely
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

Unauthorised disclosure, which includes unintentional disclosure, may be a disciplinary matter and in certain circumstances could constitute gross misconduct.

PAL's assessment and administration personnel will advise stakeholders what information is being held; why it is being held and how the information will be used and will request consent for such data usage, such information may be disseminated directly, in response to questions, or by signposting stakeholders to relevant policies and notices PAL provides its personnel with resources and further guidance and documents to support effective and secure data processing.

Providers acting on behalf of employers are responsible for the data and information they provide PAL, regarding apprenticeship and employer details.

### **Training**

All personnel are provided with data protection instruction as part of their induction process and the importance of protecting and safeguarding data is made throughout contracts, service level agreements, confidentiality agreements, conflict of interest declarations and associated policies.

Data protection will also form part of continuing professional development, where changes to legislation, updates will be provided typically via e-learning, PAL's own CPD resources and meetings.

All personnel including associates and consultants can access our Data Protection and Cybersecurity training resources, and PAL's Directors and Managers reserve the right to request personnel attend refresher training at anytime

PAL Directors have completed training in cyber security and advanced GDPR.

### **Roles and Functions**

PAL personnel only have access to the personal data they need to carry out their duties and each data agent has a line manager they can report to seek clarification or advice regarding data processing. All staff have access to all policies cited in this policy document, and additional guides which provide guidance and examples to support their understanding and application of the data protection and privacy principles, PAL's basis for data processing and data subject rights.

IT requirements and associated security arrangements are overseen by the Operations team on behalf of the PAL Board. Under the guidance of the Director of Audit and Compliance, PAL carries out a self-evaluation on a bi-annual basis that reviews our compliance to relevant regulatory requirements. **The DPO is also responsible for administering and monitoring SARs and implementing and overseeing data breach reporting.**

The PAL Board, as part of PAL's business continuity arrangements and risk management, undertake regular risk reviews, that consider all aspects of business and the integrity, probity and suitability of resources, provisions and policies and procedures.

All personnel are required to sign confidentiality agreements, which include the requirement to safeguard personal data and contracts and service level agreements and contracts assimilate such requirements.

## Data Protection by Design & Default

We have put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Voluntary appointment of a DPO, suitably senior within the organisation, as a director and therefore able to directly influence policy development and operational practice in conjunction with PAL Board colleagues
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- DPO oversees the risk register and as such can review PAL's data management capacity, capability and compliance and alert PAL Board to any risks
- Integrating data protection into this policy and related policies and supporting documentation such as the Assessment (EPA) Manual for stakeholders
- This policy detailing how to make an enquiry or complaint in respect of data processing
- Ensuring PAL personnel have access to training and information on data protection law, this policy, any related policies, and any other data protection matters
- DPO has ownership of the data breach reporting and oversight of all governance reporting activities and as such can identify and monitor trends and practices that may give rise to data management improvements or concerns
- PAL Board collective responsibility as data controller and contingencies for cover for regulatory reporting
- Data processing, data management, data accuracy included in self-evaluation activities

## Sharing your Personal Data

We will not disclose personal data to any third party unless we have a lawful basis for doing so. Confidentiality will be respected, where appropriate.

Where we share personal data with third parties, this is to enable us to comply with regulatory requirements, and or legal obligations, meet legitimate interests and deliver a service that meets our stakeholders needs and expectations.

We share personal data with trusted third parties categorised under five headings: Assessing, Consultancy, Funding, Certification, and Internal Business Systems. The entries are designed to indicate the work function each third party is associated with:

- Assessing for the provision of assessment materials, reports, and assessment outcomes accessible to Apprentices, Training Providers, to include Employer Providers and Employers via our assessment scheduling platform and email
- Consultancy for the provision of audit and compliance services
- Funding, we receive DfE funding via Providers/Employers
- Assessment outcomes, grades, results data- Ofqual for research and analysis
- Apprentice certificate via DfE
- Internal Business Systems to store and facilitate all communication, assessment reporting, and for the management and monitoring and the running of our business

Without the use of these third-party services, we would not be able to operate effectively. The policy we apply to those organisations to keep your data safe and protect your privacy:

- We provide only the information they need to perform their specific services
- They may only use your data for the exact purposes we specify in our contract/agreement with them
- We work closely with them to ensure that your privacy is respected and always protected
- If we stop using their services, any of your data held by them will either be deleted or rendered anonymous, after their specified time for holding records

We may, from time to time, move supplier. If this happens, your personal data will, where relevant, will be transferred to the new data processor in alignment with the policy mentioned above. If you require further specific information around our third parties data processors, please contact us using the information below, specifying the exact nature of the information you need to email: [info@professionalassessment.co.uk](mailto:info@professionalassessment.co.uk) and mark for the attention of the DPO.

Third parties such as Ofqual, Skills England and Dfe have data privacy notices and policies that you can access via their websites.

PAL will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects PAL personnel, and any third parties PAL representatives were engaged with at the time of the emergency.

We expect PAL personnel and those of our providers, and employers and apprentices to respect the confidentiality of information about individuals. Whilst we will support PAL personnel in taking decisions about information sharing in accordance with their professional judgement PAL may take disciplinary or legal action against those who wilfully misuse personal data for unauthorised purposes.

### **Misuse of Personal Information**

It is an offence for a person, knowingly or recklessly, without the consent of PAL to:

- obtain or disclose personal data or the information contained in personal data, or
- procure the disclosure to another person of the information contained in personal data

Unless the disclosure:

- was necessary to prevent or detect crime; or
- was required or authorised by law

PAL will act against anyone found to be supplying information to a third party or using information for their own purposes without the consent of PAL or a reasonable belief that they were not working in accordance with the wishes of PAL. Such offences are criminal offences.

### **Provider, Employer and Apprentices Responsibilities' (clients/customers)**

All third parties/customers shall:

- Ensure that all personal information which they provide to the assessment company is accurate and up-to date. **Where the Apprentice, employer or training provider provide inaccurate data and because of this, there is a need to re-certificate, or a delay in claiming an apprenticeship certificate, and additional costs are incurred, or there is a delay in payment to the AO (PAL); PAL reserves the right to charge for any financial inconvenience**
- Inform the company of any changes to that information, for example, variations of address or name, via the online management information system, which apprentices and employers will have log-in access



- Check the information which has been submitted to PAL for assessment and certification purposes, in written or automated form, and inform the assessment company of any errors or, where appropriate, follow procedures for up-dating entries via the appropriate portal. PAL will not be held responsible for errors of which it has not been informed but will work to meet data subjects rights to rectification.

## Your Rights- Access to your Personal Data

Personnel, apprentices, employers and training providers and other data subjects have the **right to be informed** and the **right to access** any personal data that is being kept about them either on a computer or in structured and accessible manual files.

Under Article 15 of the UK GDPR<sup>8</sup>, you are entitled to ask for a copy of the personal data that is held about you – this is called a Subject Access Request (SAR). When you submit a request for your personal data, you are entitled to:

- confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the following information:
- know why we have processed your personal data – the reason(s) and purpose(s) for the processing
- the categories of personal data concerned
- know if we have shared or will share your personal data and if so, with whom and for what purpose(s). In particular with recipients in third countries and international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- a copy of the personal data undergoing processing
- the existence of the right to request for rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing
- where the personal data are not collected from you, any available information as to their source
- complain to the information commissioner's office (ICO)<sup>9</sup>

### Subject Access Request (SAR)

Any person may exercise this right by submitting a request in writing to PAL's DPO, in their absence PAL's Business Operations Director or Managing Director will respond to a SAR.

We try to be as open as we can be regarding giving people access to their personal information. Individuals can find out if we hold any personal data by making a '**Subject Access Request' (SAR)**. There is no charge for such a request, and we will respond within 30 days of a verified\* request. If we do hold information about you, we will:

- give you a description of it
- tell you why we are keeping it
- tell you who it could be disclosed to
- let you have a copy of the information in an intelligible form

To make a SAR to us for any personal information we may hold, you need to put the request in writing addressing it to either:

- email: [info@professionalassessment.co.uk](mailto:info@professionalassessment.co.uk)- subject SAR<sup>10</sup>
- Or by posting to: Connect House, Kingston Road, Leatherhead, Surrey, England, KT22 7LT

***To protect the confidentiality of your information, we will ask you to verify your identity before we proceed with any request you make under this Data Protection and Privacy Policy. If you have authorised a third party to submit***

---

<sup>8</sup> See Article 15 of the UK GDPR for the full list of subject access rights

<sup>9</sup> ICO <https://ico.org.uk/>



***a request on your behalf, we will ask them to prove they have your permission to act. From the date, we receive this information we will respond within 30 days.***

We will try to deal with your request informally if you agree this is the best way to proceed, for example by providing you with the specific information you need over the telephone or by email. If we do hold information about you, you can ask us to correct any mistakes by using the same email or postal address above. PAL will ask the data subject in what format you wish to receive the information and will make best endeavours to address this requirement.

If we choose not to action your request, we will explain to you the reasons for our refusal. If we feel your application isn't covered under the definition of a SAR, we shall endeavour to assist you to the best of our ability.

PAL aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days unless there is a good reason for the delay. In such cases, the reason for the delay will be explained in writing by the DPO or in their absence the Business Operations Director or Managing Director to the data subject making the request.

SARs will be recorded and monitored by the DPO. PAL treats each SAR on its own merit.

#### **Subject Access Requests Should Include:**

- Name of individual
- Correspondence address
- Contact number and email address
- Format in which you wish to receive the information

#### **Children & Subject Access Requests**

Personal data about a child belongs to that child, and not the child's parents or carers. As a general rule only those with parental responsibility will have the right of access to information about a child's educational, medical and Children's Services record.

All data subjects, including children have the right to: be provided with a transparent and clear privacy notice which explains who you are and how their data will be processed.

Children have a right to access data so long as it's safe. Article 17 of the UNCRC says children and young people should be able to access information, particularly from the media.

#### **Responding To Subject Access Requests**

When responding to requests, we:

- Typically ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond as quickly as possible and within 30 days of the initial request- for simple requests. If the SAR is complex, we may require a longer period to respond, we will notify you within 30 days if this is the case and will advise you of the time required, which should not exceed three months
- Will provide the information free of charge

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

## Manifestly Unfounded and Excessive

For almost all the Individual Rights (excluding the right to be informed and the rights regarding automated decision making) an organisation can refuse a SAR if they reasonably believe the request is manifestly unfounded or excessive.

Manifestly unfounded examples can include:

- The requester has no real or sincere intention of exercising their right, for example if they make the request, but offer to withdraw their request in exchange for some form of benefit
- The SAR is made with malicious intent, and is being used to harass an organisation, with no other intent but to cause disruption
- The request makes unsubstantiated accusations against you or specific employees
- The individual is targeting a particular employee against whom they have some personal grudge

Excessive requests are where the requester makes several requests, which overlap previous requests, where they have had the information, they are entitled to, in the most appropriate format, but continue to persist with further requests, which substantially are the same as the original request.

PAL will review any SAR received on a case-by-case basis.

## Responding to Requests that involve others (third parties)

Where possible, PAL will consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, we would not comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

[ICO detailed guidance](#) provides further information on what you need to consider in these circumstances.

## Other Rights <sup>11</sup>

Data subjects have the following rights in relation to personal data:

**Right to rectification** – you can ask PAL to rectify any inaccuracies in your personal data and receive notification that this has been done; this includes processing carried out on our behalf by third parties, so for example in requesting the correction of your name spelling on your apprenticeship certificate. In the case of apprentices for example their Provider can request that PAL corrects any mistakes. To assist PAL, we ask any identified mistakes or inaccuracies are reported to PAL as soon as is practically possible so we can make sure our data is accurate and current.

**Right to erasure** – you can ask PAL to erase, delete or destroy any personal data we process concerning you, if you believe we have obtained the data unfairly, have misused the data and not processed the data in line with our lawful basis for processing data

**Right to restrict processing** – you can ask PAL to restrict certain personal data we process about you, for example you can ask us to stop processing your data whilst we are seeking to rectify mistakes, in this situation PAL will suppress processing. In some circumstances, you can restrict our processing of your personal data, request a machine-readable copy of your personal data to transfer to another service provider and compel us to erase your personal data if there is no other legal basis for its retention.

Where any rectification, erasure of personal data or restriction of processing is carried out in accordance with the above, GDPR regulations and this policy, PAL shall communicate any rectification, erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. You are entitled to be informed about those recipients upon request.

---

<sup>11</sup>Individual rights are subject to certain conditions see GDPR, Articles – 20

**Right to data portability** – you have the right to receive personal data held in a structured, commonly used, machine readable format (PAL does not typically or routinely process this form of data).

**Right to Object-** Where we are using consent as our lawful basis for processing your personal data (e.g., electronic communications inclusive of newsletters, industry news, similar products & services, invitations to events and surveys) you have the right to object at any time. Send your request to [info@professionalassessment.co.uk](mailto:info@professionalassessment.co.uk). Where we are using your personal data because it is in our legitimate interests to do so, you can object to us using it this way, if you object on the grounds that the processing is causing you substantial damage or distress (e.g., the processing is causing you financial loss and as such your rights override our legitimate interests).

**Rights in relation to automatic decision-making and profiling** PAL does not undertake profiling, but for multiple choice question and situational judgement tests, unless a paper-based format is requested, these tests are automatically marked. You can request access to your scores, you cannot have access to the questions and your response to each question.

**For detailed information regarding your rights, please refer to the Information Commissioner's Office (ICO) website at <https://ico.org.uk/for-the-public/>. You can also contact PAL's DPO . Note the proposed DUA may amend or enhance rights of individuals or organisations**

## Exemptions

The UK GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances.

Whether or PAL can rely on an exemption often depends on why we process personal data. PAL does not routinely rely on exemptions; and we consider them on a case-by-case basis. If PAL applies for an exemption, we will document and record our reasons for doing so. If no exemption covers what we do with personal data, we will comply with the UK GDPR regulations.

### What are Exemptions?

The exemptions in the DPA 2018 can relieve an organisation of some of its obligations for things such as:

- The right to be informed
- The right of access
- Dealing with other individual rights
- Reporting personal data breaches; and
- Complying with the principles

Some exemptions apply to only one of the above, but others can exempt an organisation's response from several things.

To access more information regarding exemptions, visit <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/exemptions/>

### Assessment Marks and Grades

Apprentices and employers shall be entitled to information about their grades for assessments and final assessment feedback and reports with the registered Training Provider having notification of results and access to pertinent reports. Grades and outcomes of assessments will be shared with the relevant provider unless the employer or apprentice provides a legitimate reason for withholding such information, however the Provider is responsible for processing their element of any claim of assessment outcomes and as such refusal to provide this information will impact PAL and the Provider and prevent PAL from receiving legitimate funds for approved assessment services, so any request to withhold information would not include results, but could include reports.

### Assessment scripts, recordings, and Assessment marks

This exemption can apply to personal data in assessment activities.

It exempts an Assessment Organisation/Awarding Organisation from the UK GDPR's provisions on:

- The right to be informed
- The right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

Apprentices and their associated third parties, employers and providers **do not have the right** to copies of the apprentices' answers in direct relation to questions and, this extends to recordings of an apprentice's responses in an interview, professional discussion or oral question and answer session. If you think your grade is wrong, you will need to pursue this via the relevant enquiries and appeal procedures.

The apprentice has the right to enquire and ask to see all their assessment grades, they do not have the right to have access to test responses, or assessment responses as provided in Q&A sessions or interviews.

Notably to provide access to recordings, scripts and assessment responses would be in contravention of qualification regulatory conditions.

**See Data Relevant Provisions in the Data Protection Act 2018 (the exemption) - Schedule 2, Part 4, Paragraph 25 for further information**

### Security and Data Security Breach Management

All personnel are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties. Access to personal data should only be given to those who need access for the purpose of their duties. All staff will comply with PAL's IT Policy.

Serious data breaches where there is a high risk to the rights of the individual will be reported to the data subject concerned and the Information Commissioner's Office (ICO) in compliance with the GDPR. All data breaches will be recorded, reported to the Directors and the DAC in their capacity of the DPO will undertake an investigation and advise the MD regarding reports to the ICO and the regulatory bodies. In the absence of the MD, the DPO will directly report any serious data breach to the ICO; and the DPO will advise PAL's Responsible Officer, the Qualifications Director of the need to report such a breach to the relevant regulatory body.

### Personal Data Breaches

#### What is a Personal Data Breach?

A personal data breach means 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 can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission; and
- Loss of availability of personal data

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper

authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

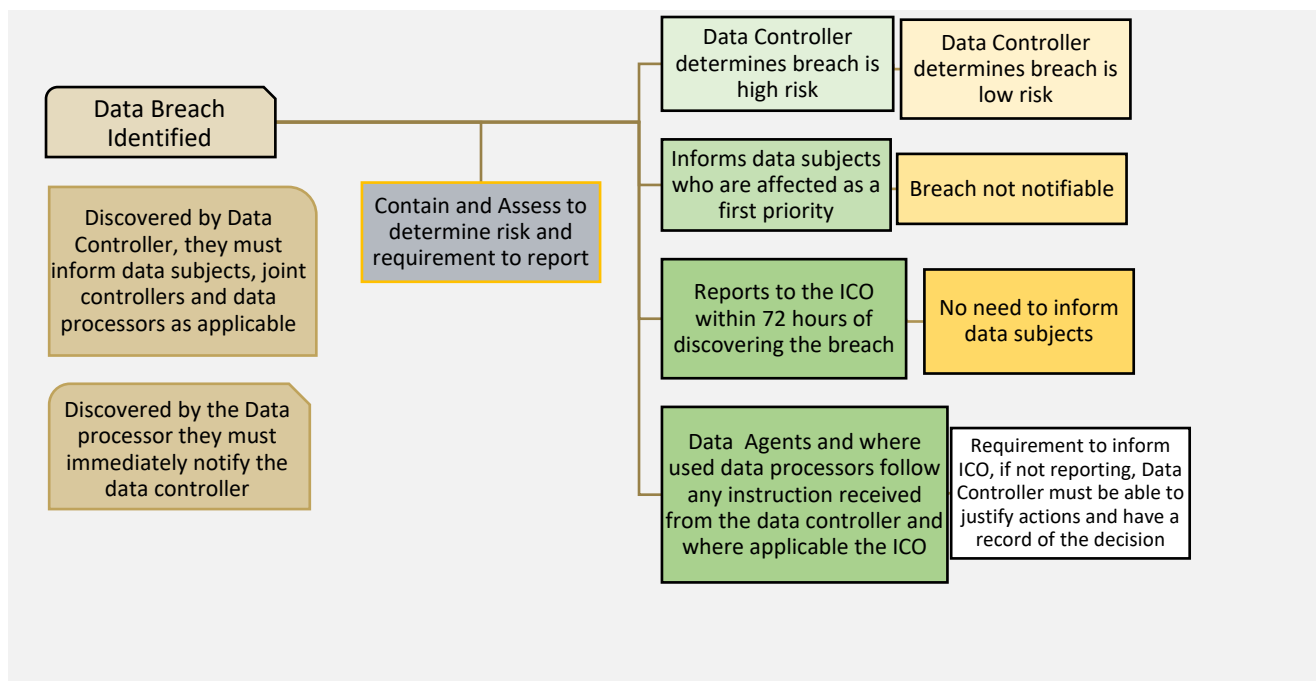
PAL will make all reasonable endeavours to ensure that there are no personal data breaches. Such breaches in an assessment context may include, but are not limited to:

- Results of an apprentice sent to the wrong employer location or wrong apprentice
- Assessment notes and feedback, left on site and accessible to others
- Inaccurate results or grade information issued
- Sharing of information/evidence provided for reasonable adjustments, to unauthorised personnel
- Sharing of information regarding a safeguarding, welfare issue to an authorised person
- Theft of a company laptop or smartphone containing non-encrypted data or information pertaining to a member of PAL personnel or third party
- Third party information, contract arrangements shared with a competitor business or other business

In the instances that a breach is a potential adverse effect or an actual adverse effect the DPO will advise PAL's RO or DRO, to facilitate reporting to the qualifications regulatory body, in line with PAL's reports adverse events procedures.

#### When does PAL need to tell Individuals about a Breach?

**If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible and to the ICO in 72 hours.**



**A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO** PAL will need to assess both the severity of the potential or actual impact on individuals because of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher. In such cases, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach, which could include for

example asking them to change their password, if the breach is in connection with data held on epaPRO or advising data subjects to look out for phishing emails or fraudulent activities on their accounts.

### **What information must PAL provide individuals when telling them about a Breach?**

PAL needs to describe, in clear and plain language, the nature of the personal data breach and, at least:

- The name and contact details of the data protection officer, or other contact point where more information can be obtained- please see DPO details
- A description of the likely consequences of the personal data breach- this will be made available from the DPO and in their absence the named deputies as already stated in this policy
- A description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects, in respect of the ICO, the Qualifications Regulator and DfE

## **Data Security**

We recognise the importance of data security and take several measures to ensure the security of personal data. These include training all staff on data protection and cyber security via an in-house training.

Access to your personal data is password-protected, and only those with permission are granted access. Any misuse of personal data by our employees, is considered a disciplinary offence and a full investigation is automatically initiated. Any misuse of data by any of our associates and consultants/technical advisors will result in an investigation and the potential termination of their service level agreements.

All personnel associated with PAL are required to sign confidentiality agreements, which refers to data protection.

Any breach of data security is recorded, and our Business Operations and Director of Audit and Compliance review our data collection and storage protocols, to ensure we only collect the data we require to discharge our services.

We conduct randomised checks on employees, associates, and consultants/technical advisors' equipment as part of our ongoing and continual improvement of organisational and technical security measures.

## **Data Retention**

The assessment company will keep different types of information for differing lengths of time, depending on legal, academic, and operational requirements. The ESFA and relevant training providers may use Apprentices' information as part of their ESFA Funding claim. Ofqual requests results data from each EPAO for research and data analysis. In both cases these organisations have strict data processing procedures that are compliant with their lawful basis for processing data and are UK GDPR compliant.

Whenever we collect or process your personal data, we'll only keep it for as long as is necessary for the purpose for which it was received. Our retention and erasure practices are set out in our data, archiving and anonymisation statement.

We retain Employer and Apprentice personal data in accordance with DfE's requirements. **DfE's<sup>12</sup> current retention period is six years after the final use of personal data related to our services and products have been rendered.**

This period of six years is stipulated by DfE, as assessment activities as undertaken by PAL are funded by and subject to potential audit by government agencies, regulatory and public bodies. We apply this retention period to any personal data relating to apprenticeship assessment activities. After seven years after the final use of your data, your data will be archived.

---

<sup>12</sup> <https://standards.education.gov.uk/standard/data-retention-and-disposal>



For non-related assessment work, to include non-assessment complaints we will retain data for no longer than three years after which time it will be erased. For compliance and audit consultancy work, any data obtained, for example, during an audit is destroyed at the end of the piece of work<sup>13</sup>.

### Complaints and Enquiries Regarding Data Processing- How to Contact PAL

Complaints and enquiries about data processing will be dealt with in accordance with PAL's Complaints Policy, email [info@professionalassessment.co.uk](mailto:info@professionalassessment.co.uk) and request the email address of the Director of Audit and Compliance (DAC), noting you have a complaint or enquiry in respect of data processing. The DAC enacting their role as the DPO will review your complaint and concerns and follow PAL's relevant procedures, in accordance with the DPA Act 2018 and the UK GDPR. Please refer to the SAR section of this policy for further information.

Alternatively, you can write to PAL's DPO (PAL's Director of Audit and Compliance) at Professional Assessment Ltd, Connect House, Kingston Road, Leatherhead, Surrey. KT22 7LT

### Contacting the regulator

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to complain with the Information Commissioner's Office (ICO). You can contact them by calling 0303 123 1113. Or go online to [www.ico.org.uk/concerns](http://www.ico.org.uk/concerns) (opens in a new window; please note we can't be responsible for the content of external websites).

### Monitoring and Review

This policy will be reviewed on an annual basis, or more frequently if there are any legislative changes that dictate the need for such a review.

### Regulatory references

PAL is required to establish and maintain compliance with regulatory conditions and criteria. This policy relates to Ofqual General Conditions of Recognition: Availability of adequate resources (retention of data) A5; Arrangements with third parties C1. This policy is designed to comply where appropriate and applicable with the DPA 2018 and any other associated regulations

Date Created: 6th July 2017

Last Review: 29<sup>th</sup> May 2025

Next Review: 29<sup>th</sup> May 2026

Person Responsible for review: Director of Audit and Compliance

This Policy has been agreed by Linda Martin, Managing Director

---

<sup>13</sup> In terms of compliance working, we do not retain any learner evidence / records. We retain the audit checklists should there be questions from the provider later. These have learner names and findings on them. These will be appropriately archived after six years. Reasons for our data approach here, is audit and compliance clients require PAL to select different learners in every audit. PAL needs to keep a track of who we have previously sampled, hence the retention of the checklists. We will always confirm with our client's data retention, removal, and archiving procedures. Audit and Compliance work involving DSATs, requires the Audit and Compliance team to have these for the current and previous funding year, which can be audited by the ESFA. The Director of Audit and Compliance is responsible for the management, protection and archiving and deleting of such data at the appropriate times.

## Appendix One-Personal Data

The UK GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
  - can be identified or who are identifiable, directly from the information in question; or
  - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are more sensitive, and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

### What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However, whether any potential identifier identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The UK GDPR provides a non-exhaustive list of identifiers, including:
  - name
  - identification number
  - location data; and
  - an online identifier.
- 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.



### **Can we identify an individual directly from the information we have?**

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

### **Can we identify an individual indirectly from the information we have (together with other available information)?**

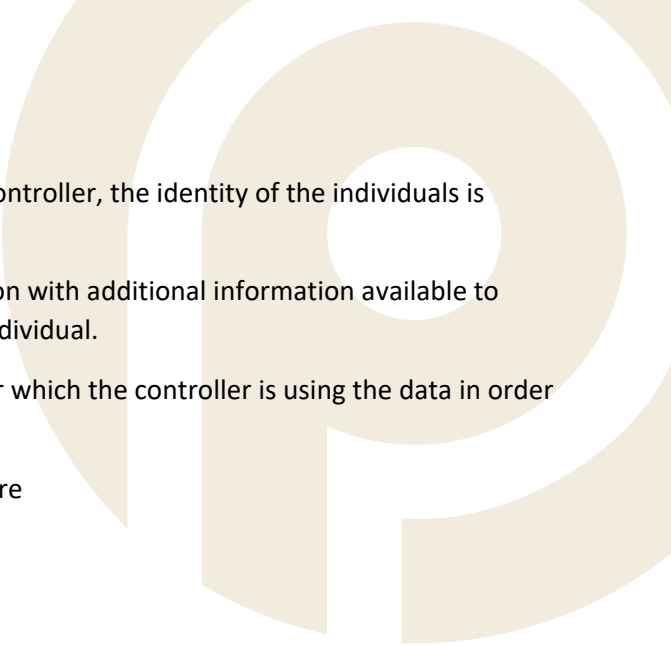
- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example because of technological developments).

### **What is the meaning of 'relates to'?**

- Information must 'relate to' the identifiable individual to be personal data.
- This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether or not data relates to an individual, you may need to consider:
  - the content of the data – is it directly about the individual or their activities?
  - the purpose you will process the data for; and
  - the results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and ensure you hold and dispose of it securely.
- Inaccurate information may still be personal data if it relates to an identifiable individual.

### **What happens when different organisations process the same data for different purposes?**

- It is possible that although data does not relate to an identifiable individual for one controller, in the hands of another controller it does.

- 
- This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant, and the data therefore does not relate to them.
  - However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.
  - It is therefore necessary to carefully consider the purpose for which the controller is using the data in order to decide whether it relates to an individual.
  - You should take care when you make an analysis of this nature

## Appendix Two -What Information we process and why

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary, or required by the regulatory bodies and government agencies and departments that regulate and audit our activities

**We hold personal data in five data subject categories.** These include Apprentices, Employers, Providers, Suppliers, and our Employees. Suppliers will receive the relevant information in the agreements we hold with them, and our Employees have internal notification not appropriate to this document. We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary, or required by the regulatory bodies and government agencies and departments that regulate and audit our activities

We may occasionally send relevant information in the form of newsletters, industry news, similar products and services, invitations to events and surveys in accordance with a data subject's preferences on an opt-in basis within our Contact Preference Centre.

### Apprentices

We process apprentice personal data to provide our assessment services. Concerning assessments, we require specific information for registration and certification with Ofqual and DfE Apprenticeship service.

For assessment services, once PAL is formerly engaged, we will require information of the apprentice and employer to facilitate assessment.

### Required information for assessments'

To enrol apprentices and certificate the outcomes of assessment, Professional Assessment requires the following:

- Provider Details
- Employer Details
- Apprentice Details
- Standard Details
- Declaration /Consent from apprentice to request apprenticeship certificate
- Notification of any perceived or actual conflicts of interest

### Provider details

	Details
Provider Name	The name of the main training provider.
UKPRN	The training provider UKPRN is automatically populated when you select their name.
Contact Details	Contact details for main point of contact to include name; job title and best method of contact (email address or phone number)

## Employer details

	Details
Employer Reference Number	The Employer Reference Number (ERN) for the learner's employer. The Employer Data Service (EDS) issues the ERN. The main provider will know this number if the employer is not privy to the information
Employer Name	The employer name, contact details, to include contact number and email and the address supplied is where the apprentice certificate will be posted to.
Employer Contact	
Employer Address	
Town/City	Mandatory address field
Post Code	Mandatory address field

## Apprentice Details

	Details
Registration Details, to include whether employer is a levy or non-levy employer	Requires Professional Assessment to specify how the apprenticeship is funded.
Unique Learner (apprentice) Number	This is the apprentice's ten-digit Unique Learner Number issued by the Learner Record Service. The main provider will know this number and will share with the relevant End-point assessment organisation (EPAO).
First Name	This is the name that will appear on the certificate.  It should be the name the apprentice registered with the main training provider to take their apprenticeship recorded in the Individualised Learner Record (ILR).
Family Name	
Date of Birth	The apprentice' date of birth.
Sex	The gender of the apprentice, based on the options provided by <u>DfE</u> .

## Standard details

	Details
Standard Code	The Standard Code <a href="#">listed on the Learning Aims Reference Service (LARS)</a> .
Level	The level of the Standard as it appears on LARS.

Option	For some Standards, the learner can take different options.
Publication Date and Version	The date the Standard was published and where applicable version number
Overall Grade	The overall grade awarded for the achievement of the Standard. For some Standards, there is no grade awarded.
Learning Start Date	The date on which the learning for the Standard began. The main provider will know this.
Achievement Date	This is the date you confirm the learner has passed the end-point assessment and achieved the Standard.

We will collect this data from the apprentice, employer, and training provider, as appropriate and all of this data is required for certification purposes.

### Children

As a company we will track when we are requesting information or accessing information for people under the age of eighteen.

The GDPR has special protection for children's personal data, particularly in the context of commercial internet services such as social networking. PAL offers online services ('information society services') to children and relies on consent to collect information about them, we may need a parent or guardian's consent to process their personal data lawfully, this is specifically relevant to the EPA aspect of the business and epaPRO (the management information system) will record and engage with employers, training organisations to acquire any such permissions.

The GDPR sets the age when a child can give their own consent to this processing at 16, however a country can select an alternative age, between the age of 13-17 for a child to give their consent. **The UK has set the age limit at 13.**

PAL will request consent from parents or guardians for the use of personal images for any apprentice under the age of 18, where such images are either commissioned or provided for marketing, PR or research purposes, or such materials are provided as evidence for assessment.

### Required information for audit consultancy

For audit and compliance consultancy work the level of data required is influenced by the nature of the commissioned work and Professional Assessment Ltd, will consult with the client as to what information is needed, the purpose of that data and how the data will be used and stored.

The subsequent service level agreements will specify the nature of any data we will require, collect and collate and store. Any data collected will be for the sole function of offering the contracted service.

### **Appendix Three- Subject Consent**

In some cases, such as the handling of sensitive information or the processing of research data, the assessment company is entitled to process personal data only with the consent of the named individual. Agreement to the company handling some specified classes of personal data is a condition of acceptance of an apprentice, employer and training organisation enrolling for endpoint assessment and a condition of employment for personnel.

The assessment company may process sensitive information about a person's health, disabilities, criminal convictions, race, or ethnic origin in pursuit of the legitimate interests of the assessment company to do so. For example, where assessment activities are undertaken with candidates under the age of 18, in contact with children, including young people and people who could be considered at risk, the company has a duty under the Children Act 1989; Safeguarding Vulnerable Groups Act (2006); Protection of Freedom Act (2012); and other enactments to ensure that personnel are suitable for the job, and apprentices are fit and ready for assessment.

Additionally, all stakeholders are treated with professional courtesy and respect, and the company demonstrates concern for all stakeholders' well-being.

The company may also require such information from company personnel for the administration of the sick pay policy, the absence policy, or the equal opportunities policy, or for course assessment.

The assessment company also asks for information from company personnel about health needs, such as allergies to specific forms of medication, or conditions such as asthma or diabetes.

In some assessment scenarios, the company may need to request such information from Apprentices, for example in endorsing a request for special considerations or the application of reasonable adjustments or to protect the individual's health and safety and well-being. The company will only use such information for its intended purpose.

The consent of the data subject will always be sought before the collection of any sensitive data as defined by the Act.

**Where providers are providing potentially sensitive information, as evidence for reasonable adjustments, PAL expects any such request is made with the full knowledge and consent of the apprentice and that only information, relevant to the request and reflective of the apprentice's current needs is made available.**

#### Appendix Four **Privacy notice digital assessment recordings webinars/events/ pre-recorded pieces to Camera**

This privacy notice explains how PAL uses any personal information we collect about you when you **attend** a virtual/online meeting, event or webinar hosted by PAL (we use the term 'meeting' to refer to both webinars and live online events in this document).

Our online meetings are hosted through Microsoft Teams using either Teams Live or Teams. Microsoft Teams is a third-party service that is not owned by PAL. Microsoft Teams is a data processor. Alternatively, if an apprentice or employer or provider wishes us to use another secure online meeting platform, PAL will support this, subject to assurance of suitable accessibility and security arrangements. Stakeholders are advised to look at pertinent platforms' privacy statements.

This privacy notice only refers to the way PAL will use your information. You should also review [Microsoft Teams privacy statement](#) which explains how Microsoft processes personal data.

All data is stored securely. Microsoft stores data held on behalf of PAL within the European Economic Area (EEA). We are continually seeking assurances from Microsoft that any processing of personal data will protect the rights and freedoms of data subjects. We will update this privacy notice with further information as and when appropriate.

#### **Why we need your information when attending meetings that may be recorded**

In all cases, we need information about you to enable your attendance at the meeting. This may be as an attendee or presenter. This will include your full name, email address and details of your organisation. We need this information to allow you to access the meeting and ensure the right people are at the right meetings.

We may also collect:

- questions posed in the meeting by attendees
- text from the associated in-meeting chat
- audio, webcam video and shared screen content of panellists
- audio, webcam video or both from attendees that participated by speaking or activating webcams as part of the meeting
- recording of the meeting where this facility is used

#### **Software for meetings**

We use either Microsoft Teams or Microsoft Teams Live for meetings. Teams allows up to 300 people per session so for many of our meetings, this software is sufficient for our needs. Indeed, it allows both PAL and attendees to speak with both having sight of audio, webcam videos and chat.

#### **Recording Assessments**

For assessment purposes and the requirement to have evidence, we do record assessment activities. Apprentices and employers are advised of the recording requirement in advance. If an apprentice or employer has a legitimate reason for PAL not to digitally record an assessment, the assessor will still be required to take notes and it will be PAL's quality team that will decide if special considerations can be applied. The regulatory body will in these cases, typically be notified of the situation and PAL's reason for not recording the assessment in accordance with the assessment plan requirements.

## **Sharing and Retention- Assessment Recordings**

Recording from assessments are held securely in PAL's apprenticeship management document files. Shared access does allow relevant PAL personnel to access evidence files for the purpose of assessment, moderation, and quality assurance.

PAL is regulated by Ofqual and as part of their external audit activities, they can and do ask to sample all forms of evidence, this includes digitally recorded evidence.

For appeals and enquiries, complaints, whistleblowing, maladministration and malpractice and reasonable adjustments and special considerations, PAL will need to potentially share such evidence with others, to perform objective and fair reviews and investigations and satisfy the regulatory conditions that govern the development, delivery, and award of apprenticeship standards. For further information regarding any of these activities, please review the relevant policy and associated privacy notice.

PAL will retain learner information for six years, for assessment records PAL will comply with its data retention and archiving guidelines, which means we will keep assessment records for three years, unless we are requested otherwise due to a change in regulatory conditions. Assessment recordings will be retained for one academic post the apprenticeship completion and then archived for two years before being deleted.

For any centre activities, please refer to PAL's Data Archiving, Anonymisation and Retention Policy.

## **Recording Webinars and Events**

For webinars and events made available to our stakeholders and the wider apprenticeship community, we do record most of these meetings. Attendees will be advised of the recording, prior to the meeting, this will be noted in invites and the host facilitator will advise all participants prior to the meeting/event starting that the webinar will be recorded. At such events we can process your data if you are on screen sharing audio, webcam video or use the chat function.

Where the meeting facility allows, delegates who wish to participate can unmute their microphone to allow them to talk and/or activate their camera. Where this is the case, we will collect an audio recording and/or video of your participation.

You can submit text questions during the webinar using the chat function. If this is on Teams, then everyone will see the information during the meeting and in any recording

We may respond to you during the meeting or after the event through calling or emailing you directly, on the contact information you have provided to PAL.

All presenters will have their image and audio captured in the recording.

For client meetings and catch-ups, we do not record the meetings, however we may share the content or aspects of any such meetings with colleagues, where such colleagues are best placed to answer any queries or provide amplification and clarification to specific questions or enquiries you have made.

Where a recording is made, this may be made available as a post-event recording of the webinar made available for all registered users to view via a dedicated link provided by the PAL host. If we intend on publishing the recording elsewhere, such as YouTube, this will be explicit in the registration details.



## **Sharing personal data within PAL- Webinar**

We may share data within PAL before and after the event in the following two specific ways:

- documents containing all questions and the chat log from the meeting will be downloaded by the PAL host to provide answers to delegates' queries, to ensure completeness in any follow-ups or gaining more information for a particular question, or questions, the host may direct specific queries to individuals at PAL, who were not necessarily in attendance at the webinar
- the attendee list will be provided before and after the event to the PAL Board, firstly to facilitate feedback and secondly to ascertain the take-up and effectiveness of such webinars or events

## **Legal basis for processing**

Our processing of the data is necessary for PAL to deliver our services made available to you and meeting our legitimate interests. Where we process special category data such as in respect of any access requirements, we do this with your explicit consent. You can waive accessibility rights, or request PAL provides the information in a different format, so you can access the information. PAL will endeavour to meet such requests where practically possible.

If you wish to withdraw from an event, ideally please contact PAL at [info@](mailto:info@) to notify us of your cancellation.

## **Retention of recordings webinars and events**

We will review recordings on a yearly basis to see whether the information is still required. We will only keep recordings where the topic is relevant and has been made available via a dedicated link. In most cases, this will be no more than 2 years.

On occasion, we might record a piece to camera in the form of an interview, where a member of the PAL team interviews a guest speaker, and this is undertaken as a piece to camera. Alternatively, we may disseminate talking heads videos, that involved PAL personnel and selected stakeholder representatives. Prior to such recordings we will seek consent from any guest speaker. These types of recordings will be made available either via our website or Padlets.

We will review these specific recordings every 6 months although we would expect such recordings to be available for at least 2 years.

## **Your rights, e.g., access, rectification, erasure**

Subject to some legal exceptions, as a data subject, you have the legal right to:

- access personal data relating to you
- have all or some of your data deleted or corrected
- prevent your personal data being processed in some circumstances
- ask us to stop using your data, but keep it on record

Further details of the rights available to you and how you can exercise these can be found in PAL's Data Privacy Notice and Data Protection and Privacy Policy, available via the PAL website.

## **How to contact us regarding the privacy notice for attending recorded events**

Please send us an email at [info@professionalassessment.co.uk](mailto:info@professionalassessment.co.uk) and use the following subject lines:

- "Attending a recorded event" if your query is about the privacy notice for attending a recorded event

- “Data protection officer” if your query is regarding retention or removal of your personal data.

We will respond to any rights that you exercise within 30 days of receiving your request, unless the request is particularly complex, in which case we may require longer. We will inform you of this should it be the case.

If you are dissatisfied with our response, you can complain to the Information Commissioner’s Office:

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to complain with the Information Commissioner’s Office (ICO). You can contact them by calling 0303 123 1113. Or go online to

[www.ico.org.uk/concerns](https://www.ico.org.uk/concerns) (opens in a new window; please note we can't be responsible for the content of external websites).

### **Further information**

The privacy notice for recordings is available as an appendix in our Data Protection and Privacy Policy, as well as being available as a separate document. You can use our info@ email address to request a copy of this specific notice, please indicate in the subject header you wish to have a copy of PAL’s Privacy notice digital assessment recordings webinars/events/ pre-recorded pieces to Camera

Please note, where we do not specify the exact audience for our meetings or events, we do however indicate suitability and who might benefit from attendance.

## Appendix Five Data (Use and Access) Bill Overview

The Data (Use and Access) Bill [HL] aims to enhance data access and usage across various sectors to boost the UK economy, improve public services, and simplify citizens' lives. Introduced in the House of Lords on 23 October 2024, it has progressed through various stages and had its second reading in the House of Commons on 12 February 2025.

### Objectives of the Data Bill

The government outlines three primary objectives for the bill:

- Growing the economy
- Improving UK public services
- Making people's lives easier
  - The bill is projected to boost the UK economy by £10 billion and free up millions of hours for police and NHS staff.

### Structure and Key Parts of the Bill

The bill consists of eight parts, each addressing different aspects of data use and access:

- Part 1: Access to customer and business data, expanding "smart data" beyond finance.
- Part 2: Regulation of digital verification services through a trust framework.
- Part 3: Establishment of a national underground asset register.
- Part 4: Transition from paper-based to electronic registration of births and deaths.
- Part 5: Revisions to the UK's data protection regime.
- Part 6: Abolishment of the Information Commissioner's Office, transferring functions to a new body.
- Part 7: Provisions for health, social care, smart meters, public service delivery, and online safety.
- Part 8: Final provisions regarding amendments and regulations.

### Economic Impact of Data

The UK data economy was estimated to represent 7.4% of GDP in 2023, with data-driven companies contributing £84.9 billion to the economy in 2022. The bill is expected to yield net benefits between £3.2 billion and £18.8 billion over ten years, with a best estimate of £10 billion.

### Previous Conservative Government Bills

The Data (Use and Access) Bill follows two previous bills from Conservative governments that aimed to reform data protection laws. Both earlier bills were withdrawn or did not progress, with the latest bill reflecting a commitment to data-driven public services while ensuring strong safeguards.

### Reactions and Concerns Regarding the Bill

The bill has received mixed reactions:

- The Information Commissioner's Office supports the bill as pragmatic and proportionate.
- Tech UK views it as a significant step in modernizing data protection.

- The Open Rights Group and Big Brother Watch express concerns about potential threats to privacy and data protection rights, particularly regarding AI and law enforcement data sharing.

### **Right to Data Portability and Smart Data**

The UK GDPR grants individuals the right to data portability, allowing them to access and reuse their personal data across different services. Smart data extends this right by enabling secure data sharing with authorized third-party providers for enhanced services and competition.

- Article 20 of the UK GDPR provides individuals with the right to data portability.
- Smart data allows consumers to share data with authorized third-party providers (ATPs) for innovative services.
- Open Banking is the only current example of a smart data scheme, with over 10 million users.
- The government aims to establish a legislative framework for smart data to enhance data portability rights beyond the current GDPR provisions.

### **Legislative Framework for Smart Data**

The proposed bill aims to create a robust framework for smart data schemes, replacing outdated regulations and addressing the evolving needs of data sharing. It seeks to improve data portability, enhance competition, and empower consumers.

- The bill will replace sections 89-91 of the Enterprise and Regulatory Reform Act 2013.
- It aims to facilitate long-term continuation of open banking and extend its benefits to an open finance scheme.
- The government acknowledges that existing regulations are insufficient for effective smart data schemes.
- The bill's provisions are designed to improve data portability between suppliers, service providers, customers, and third parties.

### **Definitions and Key Terms in the Bill**

The bill defines key terms such as "business data," "customer data," and "data holder," establishing a clear framework for data sharing and responsibilities. These definitions are crucial for implementing the proposed regulations effectively.

- "Business data" includes information about goods, services, and customer feedback.
- "Customer data" refers to information related to a customer's transactions and interactions with a trader.
- A "data holder" is defined as the trader or a person processing data on behalf of the trader.
- The bill clarifies that a customer can be anyone receiving goods or services, not just the purchaser.

### **Regulations for Customer Data Sharing**

The bill empowers the Secretary of State or Treasury to create regulations requiring data holders to provide customer data to customers or authorized persons. This aims to enhance consumer control over their data and improve service offerings.

- Regulations will require data holders to provide customer data upon request from customers or authorized persons.

- The bill allows for the collection, retention, and rectification of customer data to ensure accuracy.
- Authorized persons may act on behalf of customers, enabling services like account management and negotiation for better deals.
- The Secretary of State must consider the impact of regulations on customers, data holders, and competition.

### **Business Data Regulations and Provisions**

The bill also includes provisions for business data, allowing for its publication and sharing without requiring customer authorization. This aims to enhance transparency and competition in the marketplace.

- Regulations may require data holders to publish business data or provide it to specified third parties.
- Business data does not directly relate to individual customers, allowing for broader access.
- The bill mandates that data holders maintain specific business data to support smart data schemes.
- The Secretary of State must consider the effects of regulations on small businesses and innovation.

### **Decision-Making and Compliance Framework**

The bill outlines the role of decision-makers in authorizing data sharing and ensuring compliance with regulations. This framework is essential for maintaining accountability and protecting consumer rights.

- Decision-makers will be responsible for authorizing third-party recipients of customer data.
- Regulations may require decision-makers to monitor compliance and handle complaints.
- The bill ensures that affected persons have rights to review decisions and appeal to courts.
- Decision-makers can suspend or revoke authorizations based on compliance issues.

### **Interface Bodies and Their Functions**

The bill proposes the establishment of interface bodies to facilitate data sharing and set standards for data interfaces. These bodies will play a crucial role in ensuring the smooth operation of smart data schemes.

- Interface bodies will establish and manage data sharing interfaces and standards.
- Regulations may require data holders to set up interface bodies to enhance data sharing.
- Monitoring powers will be conferred on interface bodies to ensure compliance with standards.
- The Open Banking Implementation Entity serves as a model for these interface bodies.

### **Enforcement and Compliance Mechanisms**

The bill includes provisions for monitoring and enforcing compliance with smart data regulations. This ensures that data holders and third-party recipients adhere to the established rules.

- Public authorities will be designated as enforcers to monitor compliance with regulations.
- Enforcers will have powers to investigate, issue compliance notices, and impose financial penalties for non-compliance.
- Regulations may create offences for providing false information to enforcers.
- Enforcers can publish statements regarding non-compliance to promote accountability.

## **Financial Provisions: Fees and Levies**

The bill allows for the imposition of fees and levies to fund the operations of smart data schemes, ensuring that costs are covered without burdening taxpayers. This financial framework is essential for the sustainability of the initiatives.

- Fees may be charged to data holders, decision-makers, and enforcers to cover operational expenses.
- Levies can be imposed on data holders and third-party recipients to fund regulatory functions.
- The regulations will specify how fees and levies are determined and managed.
- Financial assistance may be provided as a backstop to ensure the self-financing of smart data schemes.

## **Role of the Financial Conduct Authority (FCA)**

The FCA will play a significant role in regulating financial services interfaces under the smart data framework. This ensures consistency and compliance across the financial services sector.

- The Treasury can enable the FCA to set rules for financial services providers regarding data sharing interfaces.
- FCA rules will ensure that financial services smart data schemes align with open banking standards.
- The FCA can impose penalties and levies to recover expenses related to its regulatory functions.
- Coordination with other regulators will be facilitated to enhance oversight of financial services.

## **Review and Oversight of Regulations**

The bill mandates regular reviews of the regulations to ensure their effectiveness and relevance. This oversight is crucial for adapting to changing market conditions and consumer needs.

- The Secretary of State and Treasury must conduct reviews of part 1 regulations every five years.
- Reports on the findings of these reviews will be published and laid before Parliament.
- The reviews will assess whether the regulations remain appropriate and effective.
- Joint reviews may be conducted for provisions made by both the Secretary of State and Treasury.

## **Conclusion and Industry Reactions**

The ICO and industry stakeholders have expressed support for the bill, highlighting its potential to empower consumers and foster innovation. However, some caution that the bill alone will not achieve its goals without effective implementation.

- The ICO welcomes the bill for enhancing consumer control over personal information.
- Industry leaders anticipate collaboration to utilize the bill's provisions effectively.
- Concerns exist that the bill provides a framework but requires active policymaking to realize its potential.
- The bill is seen as a significant step towards establishing smart data initiatives across various sectors.

## **Digital Verification Services Regulatory Framework**

The UK government is establishing a regulatory framework for digital identity verification services to ensure security and trustworthiness without a centralized scheme. This framework will include a Trust Framework, a public register of certified providers, and an information gateway for data sharing.

- The framework aims to support private providers in demonstrating security and trustworthiness.
- A Trust Framework will set standards for data privacy, security, and inclusion.
- A public register will list certified digital verification service (DVS) providers.
- An information gateway will allow public authorities to share data with certified DVS providers.
- The framework is based on previous consultations and aims to prevent fraud and improve efficiency.

### **Importance of Identity Verification**

Identity verification is crucial for accessing various services in both physical and digital environments. Traditional methods are often inefficient and prone to fraud, prompting a shift towards digital solutions.

- Identity verification is necessary for tasks like opening bank accounts and accessing government services.
- Traditional methods rely on physical documents and personal details, which can be costly and inefficient.
- Digital identity solutions aim to reduce fraud and streamline verification processes.

### **Digital Identities and Their Use**

Digital identities represent individuals online, allowing for secure verification during transactions. They can be single-use or reusable, enhancing privacy by allowing users to share only necessary information.

- Digital identities can be created for specific interactions or reused across multiple services.
- Users can share only the necessary attributes for verification, enhancing privacy.
- The government promotes digital identities to support inclusion for those lacking traditional documents.

### **Consultations and Stakeholder Feedback**

The government has conducted consultations to gather insights on digital identity systems, with mixed responses from privacy advocates and industry stakeholders. Concerns include potential surveillance and the need for strong privacy protections.

- The Conservative government sought evidence on improving identity verification through consultations.
- Privacy groups raised concerns about data misuse and surveillance risks.
- Stakeholders emphasized the need for legal certainty and clear governance in digital identity systems.

### **Trust Framework Development and Governance**

The UK digital identity and attributes trust framework is being developed to establish standards for digital verification services. The Office for Digital Identities and Attributes (OfDIA) will oversee the framework and its implementation.

- The trust framework will set standards for DVS providers, ensuring compliance with existing legislation.
- OfDIA will manage the certification process and maintain the public register of certified providers.
- The framework aims to build trust and facilitate accurate identity verification.

### **Cybersecurity and Data Protection Measures**

Cybersecurity is a critical concern for the National Underground Asset Register (NUAR), which will manage sensitive data about underground assets. The government is committed to ensuring robust security measures are in place.

- The NUAR will be developed with input from the National Cyber Security Centre to protect sensitive information.
- Guidance on cybersecurity measures will be provided to stakeholders accessing the NUAR.
- The potential misuse of data could have serious implications for critical infrastructure.

### **National Underground Asset Register Implementation**

The National Underground Asset Register (NUAR) aims to improve data sharing about underground assets to prevent accidental strikes during excavation. Legislation will require asset owners to upload data to the NUAR.

- The NUAR will be a digital map of underground assets in England, Wales, and Northern Ireland.
- Asset owners will be legally required to upload information to the NUAR to ensure comprehensive data availability.
- The government estimates that the NUAR could prevent 15% of accidental asset strikes, improving safety and efficiency.

### **Reform of Births and Deaths Registration Process**

The bill proposes significant reforms to the registration of births and deaths in England and Wales, transitioning from a paper-based system to an electronic one. This change aims to streamline the registration process and improve access to records for registrars and the Registrar General.

- Clause 61 amends the Births and Deaths Registration Act 1953 to allow electronic registration, eliminating the need for paper registers.
- The Registrar General will have the authority to determine the format of registers and ensure immediate access to entries.
- Provisions for quarterly returns and paper storage requirements will be repealed.
- Local authorities must provide necessary equipment for registrars to perform their duties.
- The bill maintains existing requirements for the custody of current paper registers until the new system is implemented.

### **Data Protection and GDPR Amendments**

The bill introduces amendments to the Data Protection Act 2018 and the UK GDPR, focusing on the processing of personal data, especially for research and statistical purposes. These changes aim to balance data protection with the needs of scientific research and public interest.

- Part 2 of the Data Protection Act 2018 governs personal data processing, detailing responsibilities of data controllers and processors.
- Clause 67 defines scientific research and statistical purposes, ensuring that processing for these purposes is in the public interest.
- The bill introduces a public interest test for scientific research, requiring that research must benefit society.
- New provisions clarify consent requirements and lawful grounds for processing personal data, including a new ground for recognized legitimate interests.
- The bill allows for the Secretary of State to amend conditions for processing special categories of data through regulations.



## **Automated Decision-Making Regulations**

The bill revises the regulations surrounding automated decision-making, aiming to provide clarity and flexibility while ensuring protections for individuals. This includes new provisions for significant decisions made through automated processes.

- Clause 80 replaces existing restrictions on automated decision-making, allowing it under broader conditions as long as safeguards are in place.
- New articles outline the requirements for meaningful human involvement in significant decisions and prohibit the use of special categories of data without explicit consent.
- The Secretary of State is granted powers to define what constitutes meaningful human involvement and significant decisions.
- The bill aims to balance the benefits of automation with the need for individual protections against harmful decisions.

## **Enhanced Protections for Children's Data**

The bill introduces specific provisions to enhance the protection of children's personal data, particularly in online services. This aims to ensure that children's rights and privacy are prioritized in digital environments.

- Clause 81 amends article 25 of the UK GDPR to require online service providers to consider children's specific needs and risks when designing their services.
- Information society services must implement measures that protect children, acknowledging their lesser awareness of data risks.
- The new duty applies to services likely to be accessed by children, reinforcing compliance with existing age-appropriate design codes.
- The amendment aims to hold organizations accountable for safeguarding children's data rights in the digital space.

## **Changes to Data Subject Rights and Requests**

The bill proposes changes to how data subject requests are handled, aiming to streamline processes while maintaining individual rights. This includes adjustments to response times and the handling of excessive requests.

- Clause 75 allows data controllers to refuse or charge fees for manifestly unfounded or excessive requests.
- Clause 76 changes the response time for subject access requests, allowing for extensions and pauses for clarification.
- New provisions clarify the information that must be provided to data subjects and introduce exemptions for disproportionate efforts in research contexts.
- The bill aims to balance efficiency in data processing with the rights of individuals to access their personal data.

## **Provisions for Research Data Processing**

The UK GDPR and the 2018 Act provide specific provisions for processing personal data for research purposes, emphasizing the importance of scientific and historical research. These provisions include data protection principles, conditions for processing special category data, and exemptions from individuals' rights.

- Three broad types of research-related purposes: archiving in the public interest, scientific or historical research, and statistical purposes.
- Article 89 of the UK GDPR mandates appropriate safeguards to protect individuals' rights during data processing.
- Data minimization is emphasized, with a focus on anonymizing or pseudonymizing data where possible.
- Section 19 of the 2018 Act adds safeguards, stating that processing cannot cause substantial damage or distress, except for approved medical research.

### **National Security Exemptions in Data Processing**

Clause 88 of the bill introduces exemptions from certain data protection provisions for national security purposes. This aims to streamline data processing for competent authorities and intelligence services.

- Exemptions may apply to data protection principles, rights of data subjects, and various enforcement provisions.
- The bill ensures that competent authorities have the same exemptions as organizations under the UK GDPR.
- This change is intended to facilitate joint operational working between law enforcement and intelligence services.

### **Joint Processing by Authorities**

Clause 89 allows for joint processing of personal data by designated competent authorities and intelligence services for national security purposes. This aims to enhance operational partnerships in response to national security threats.

- The Secretary of State can designate competent authorities as "qualifying competent authorities."
- Joint processing will be subject to controls and safeguards outlined in part 4 of the 2018 Act.
- The government aims to address challenges posed by different data protection regimes for law enforcement and intelligence services.

### **Role and Responsibilities of the Information Commissioner**

Clause 91 amends the role of the Information Commissioner, emphasizing the need for appropriate data protection while considering public interest. The Commissioner will have new duties and reporting requirements.

- The Commissioner must secure an appropriate level of protection for personal data and promote public trust.
- New duties include promoting innovation, competition, and safeguarding public security.
- The Commissioner is required to prepare and publish a strategy for discharging functions and report on compliance with duties.

### **Amendments to Codes of Practice**

Clause 92 ensures that all codes of practice follow the same parliamentary process and legal effects. The Commissioner must establish a panel of experts for input on these codes.

- The Commissioner must prepare impact assessments for all codes of practice.

- The panel will provide recommendations, and the Commissioner must explain any deviations from these recommendations.
- The Secretary of State can modify the requirement for a panel for certain codes.

### **Handling Excessive Requests to the Commissioner**

The bill introduces measures to address manifestly unfounded or excessive requests made to the Information Commissioner. This aims to streamline the Commissioner's workload and improve efficiency.

- New provisions require the Commissioner to assess performance and report annually.
- The Commissioner can prepare and publish an analysis of performance using key performance indicators.
- This aims to enhance accountability and transparency in the Commissioner's operations.

### **Notices and Penalties from the Commissioner**

The bill amends the powers of the Information Commissioner regarding notices and penalties for non-compliance with data protection laws. This aims to strengthen enforcement capabilities.

- The Commissioner can require specific documents and reports when issuing information notices.
- The time limit for issuing penalty notices is extended under certain circumstances.
- The bill allows for more flexible enforcement actions to ensure compliance.

### **Annual Reporting on Regulatory Actions**

The bill mandates the Commissioner to publish an annual report detailing regulatory actions and enforcement powers exercised. This aims to enhance transparency and accountability.

- The report must include information on investigations and enforcement actions related to law enforcement and intelligence services.
- The Commissioner must disclose the number of penalty notices issued beyond the six-month limit and the reasons for delays.

### **Changes to Direct Marketing Regulations**

The bill proposes amendments to the Privacy and Electronic Communications Regulations (PEC Regulations) to enhance privacy rights in electronic communications. This includes stricter rules on unsolicited direct marketing.

- The definition of electronic communications is clarified to include all forms of messaging.
- New consent requirements for direct marketing are established, emphasizing the need for explicit consent.
- The bill aims to reduce the number of cookie consent pop-ups and improve user experience.

### **Enhancements to Cookie Regulations**

The bill introduces new provisions regarding the use of cookies and similar technologies, aiming to streamline consent processes and enhance user privacy.

- Organizations must provide clear information about cookie usage and obtain consent.
- New exceptions for statistical information collection and user preferences are introduced.
- The Secretary of State can amend cookie consent requirements after consulting with the ICO.

## **Smart Meter Communication Services Regulations**

The bill includes provisions for the regulation of smart meter communication services, allowing for more flexible licensing processes.

- Ofgem will have the authority to grant smart meter communications licenses on a competitive or non-competitive basis.
- This aims to ensure timely appointment of successor licensees and improve service delivery.

## **Information Sharing for Public Services**

The bill amends the Digital Economy Act to facilitate information sharing for improving public services, extending this capability to businesses.

- The aim is to enhance access to government services and support for businesses.
- This change is intended to improve the efficiency of public service delivery.

## **Data Preservation for Child Investigations**

The bill mandates social media companies to preserve relevant personal data of deceased children for investigations, ensuring data remains accessible during inquiries.

- This provision aims to support coroners and investigators in accessing necessary information.
- It prevents routine data deletion during active investigations.

## **Research on Online Safety Matters**

The bill allows the Secretary of State to require regulated service providers to share information for independent research on online safety.

- This aims to enhance understanding and inform policy decisions regarding online safety.
- Ofcom will oversee the implementation of this research framework.

## **Amendments on Copyright and AI**

The bill introduces amendments to address copyright issues related to AI training, focusing on transparency and rights for copyright holders.

- Operators of web crawlers must comply with UK copyright law and disclose their identity and purpose.
- Copyright owners can claim damages for non-compliance with transparency obligations.

## **Technical Solutions for Personal Data**

The bill includes provisions for defining core personal attributes and associated metadata to ensure consistency across government data collection.

- This aims to improve the accuracy and reliability of data collected for research and evaluation.
- The Secretary of State is tasked with establishing these definitions through regulations.

## **Current Legal Framework on Intimate Image Abuse**

The existing laws regarding intimate image abuse are fragmented and do not specifically address the creation of deepfake images. The Sexual Offences Act 2003 outlines various offences related to sharing and taking intimate images without consent but lacks a direct provision for creating deepfake images.

- Section 66B of the Sexual Offences Act 2003 addresses sharing or threatening to share intimate images without consent.
- The act includes offences for taking intimate images without consent but does not cover the creation of deepfake images of adults.
- The Law Commission's 2022 report highlighted the need for new offences but concluded that merely creating deepfake images without sharing them was not sufficiently harmful to warrant criminalization.

### **Calls for Legislative Change**

There have been persistent demands for new laws to criminalize the creation and solicitation of deepfake intimate images. Advocates argue that the current legal framework fails to protect individuals, particularly women and girls, from the threats posed by deepfake technology.

- Clare McGlynn emphasized that deepfake images represent an "invisible threat" to women and girls, instilling fear and anxiety.
- Campaigns, such as one led by Jodie, have gathered significant public support, with over 69,000 signatures calling for legal changes.
- The need for legislation is underscored by personal testimonies of individuals affected by deepfake image abuse.

### **Recent Legislative Efforts and Proposals**

The Criminal Justice Bill 2023-24 initially did not include provisions for deepfake images but later proposed amendments to address this issue. The government has shifted towards a consent-based approach for new offences related to deepfake images.

- The Criminal Justice Bill introduced a framework for offences related to taking intimate images without consent but initially excluded deepfake creation.
- Following debates, the government announced plans to criminalize the creation of sexually explicit deepfake images, responding to growing public concern.
- The Non-Consensual Sexually Explicit Images and Videos (Offences) Bill proposed consent-based offences, gaining cross-party support in the House of Lords.

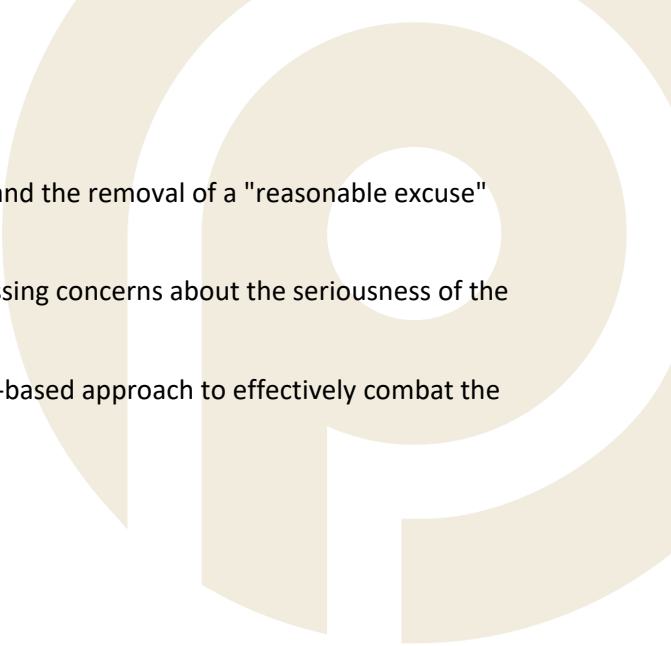
### **Details of Clause 141 in the Bill**

Clause 141 introduces two new offences related to the creation and solicitation of purported intimate images without consent. This clause aims to provide clearer legal protections against deepfake image abuse.

- The new offences include intentionally creating or soliciting the creation of a purported intimate image without consent.
- A "purported intimate image" is defined as an image that appears to show a person in an intimate state but is not a genuine photograph or film.
- The offences are summary only, with a maximum penalty of six months imprisonment or an unlimited fine.

### **Government's Response to Legislative Amendments**

The government has faced challenges in the House of Lords regarding the proposed offences, leading to significant amendments to the original clause. The final wording reflects a consensus on the need for a consent-based approach to protect victims.

- 
- Amendments included the addition of a solicitation offence and the removal of a "reasonable excuse" defence.
  - The final clause allows for imprisonment as a penalty, addressing concerns about the seriousness of the offences.
  - The government acknowledged the importance of a consent-based approach to effectively combat the creation of intimate deepfakes.