# **Logo Description automatically generated**Imparta Data Protection Policy

Version 1.6

Updated May 2024

## Contents

Imparta Ltd

522-524 Fulham Broadway

London

SW6 5NR

+44 (0) 207 610 8800

[Contents 1](#_Toc144300053)

[**1.** Imparta Data Protection Policies 3](#_Toc144300054)

[**2.** Introduction 4](#_Toc144300055)

[2.1 Summary for Employees 5](#_Toc144300056)

[**3.** Data Protection Principles 8](#_Toc144300057)

[**4.** Personal Data held by Imparta and Lawful Basis for Processing 10](#_Toc144300059)

[**5.** Imparta as Data Controller and Data Processor, Definitions and Responsibilities 11](#_Toc144300061)

[**6.** Individual Rights under the GDPR and How We Comply 14](#_Toc144300063)

[**7.** Accountability and Governance 20](#_Toc144300072)

[**8.** Storage and Transmission of Personal Data 23](#_Toc144300077)

[**9.** Incident Reporting 25](#_Toc144300081)

[**10.** Access to, and Disclosure and Transfer of, Personal Data 26](#_Toc144300082)

[**11.** Compliance and Updates 28](#_Toc144300087)

[Annexe 1: Privacy Policy Contents 29](#_Toc144300088)

[Annex 2: Archiving Policy 31](#_Toc144300089)

## Imparta Data Protection Policies

**This document details the Data Protection Policies of Imparta Ltd and Imparta Inc. (the Company, we, our) and applies in addition to all policies and provisions in our Imparta Employee Handbook (including those relating to confidentiality and information security).**

This Policy applies to all of Imparta Ltd.’s and Imparta Inc.’s employees, contractors, faculty, associates and offices whose work involves processing personal data. All such data users must comply with this policy when processing personal data on our behalf. Any breach of this Policy may result in disciplinary action.

This policy is not part of any employee’s employment contract and may be amended at anytime. However, every employee must comply with it, and any breach may result in disciplinary action.

Imparta’s Executive Team may review the Policy and any necessary revision made within 12 months of the latest revision or earlier as necessary. Imparta’s executive team is committed to continually improving our information security and data protection policies.

All new employees shall receive induction in our Data Protection, IT and Information Security Policies. Please inform your line manager or the Data Protection Officer if you do not receive this or require further training.

#### If you have any questions about this Data Protection Policy, please refer to the Data Protection Officer (Mark Abell).

## Introduction

At Imparta, we use information about individuals in our day-to-day business activities. This includes information about customers, faculty, business contacts, suppliers and employees. This Policy describes how this data must be collected, handled, and stored to meet the Company’s data protection standards and comply with the law.

This Data Protection Policy seeks to ensure that Imparta:

* Complies with UK GDPR and EU General Data Protection Regulations (GDPR).
* Protects the individual rights of staff, customers and partners.
* Is open about how it stores and processes personal data.
* Protects itself from the risks of a data breach.

The Executive Team is responsible for ensuring that Imparta meets its legal obligations. However, each team that handles personal data must ensure that it is handled and processed in line with this Policy and the data protection principles outlined.

The GDPR applies to processing carried out by organisations operating within the EU and UK. It also applies to organisations outside the EU and UK that offer goods or services to individuals in the EU and UK.

The Company may be fined substantial amounts of money for breaches of GDPR. As importantly, as data controllers, our clients will require us to be fully compliant at all times. They trust us with their data and are also at risk of fines if there are breaches.

We have appointed a data protection officer to oversee our compliance and assist our clients in understanding our GDPR compliance. The Data Protection Officer is your first point of call if you have any questions or concerns about how you should be processing, managing, storing, or transferring data and, indeed, any other data-related questions.

The Data Protection Officer (Mark Abell) is responsible for:

* Keeping the Executive Team updated about data protection responsibilities, risks and issues.
* Reviewing all data protection procedures and related policies on at least an annual basis.
* Arranging data protection advice and training for the people covered in this Policy.
* Induction training around this Policy.
* Handling data protection questions from staff and anyone covered by this Policy.
* Dealing with requests Imparta receive to see the data (subject access requests).
* Checking and approving any contracts or agreements with third parties that may handle sensitive personal data.

Others in the company also have direct responsibilities to ensure our GDPR compliance.

The Head of Information Technology Services is responsible for:

* Ensuring all systems, services and equipment for storing data meet acceptable security standards.
* Performing regular checks and scans to ensure security hardware and software function properly.
* Evaluating any third-party services the company is considering using to store or process data, for instance, cloud computing services.

The Head of Marketing is responsible for:

* Approving any data protection statements attached to communications and emails.
* Ensuring all marketing initiatives abide by marketing principles.

### 2.1 Summary for Employees

This is quite a lengthy document detailing how we meet our GDPR obligations. For ease, here is a summary of what you need to know and do to meet Imparta’s data protection requirements. This does not mean you should not read this document, but should make it more accessible to you in terms of knowing the actions you need to take.

#### Collecting personal data from clients

* Only ask for or accept personal data that is absolutely needed for the purpose at hand. Data should be limited to the data sets you need, typically names and email addresses, and the client should remove other data relating to the individual before passing it to you.
* Ask the client to send the data to you through Microsoft Teams for security. If they cannot, they can send it in a password-protected form, notifying you of the password in a separate communication.
* Never accept sensitive personal data relating to any individual’s financial details, health, politics, or sexual orientation. Typically, the only personal data we should be dealing with at Imparta are the names and business emails of training participants, along with similar information for our contacts at the client.

#### Storing Personal Data

* Client personal data, including delegate list, faculty assessment results, etc, should be primarily stored on our ILS platform on i-Coach. I-Coach is hosted on Microsoft’s secure Azure platform. Personal data may also be kept on SharePoint when working on a project that cannot be completed in ILS. This data should be deleted when no longer needed.
* Sales, marketing and finance information should be held on Salesforce/Hubspot.
* If you need to hold personal data outside ILS or Salesforce on SharePoint, only use the ‘0’ folder marked Confidential in the client folder. Personal Data in your client folders has access limited to those who need it. IT can help you with this if you have questions.
* Never print off personal data and leave hard copies lying around.
* Treat all personal data as confidential under the terms of your NDA.
* Observe retention policies in this document; if you are unclear, check in with your manager or Imparta’s Data Protection Officer.

#### Processing Personal Data

* Only process data at the direct written request of a data Controller (Client), for example, to carry out the activities requested by a client in a SOW. Never process personal data at the request of a third party.
* Get written (Sow) requests for all data processing activities, such as i-Coach registrations and assessment projects. Never pass over data before a GDPR-aligned contract and SOW is in place.
* Only use data for the purpose for which it was collected. Tell the Data Protection Officer if you think the client is asking you to use data unfairly or in a way that does not align with what the data subjects expect.
* Never use personal data for any other use than it was collected for.
* Never put different client’s data in the same folders.

#### Disclosure/Sharing

* Never send data on UK or EU individuals outside the UK or EU without the Controller's (client) permission and speaking to the Data Protection Officer
* Use Microsoft Teams to share data and confidential information where possible.
* Ensure the client’s contract allows sharing data with faculty or translators before sharing. If not, seek written permission from the client.
* All faculty, translators, contractors or other associates must be under Imparta’s NDA before being given personal data.
* Do not include delegate lists in workshop boxes – use secure digital solutions such as Microsoft Teams. Confirm with faculty that they have deleted data lists after workshops.
* Use password protection on documents with personal data in them if you have to use email.
* If clients question your diligence with personal data, remind them politely that we are under a contractual obligation with them to be secure and meet GDPR rules.

#### Retention/Disposal

* Personal information should be deleted from all systems on request from a Controller (client) or if a project ends and there is no likelihood of the data being needed again. All personal data will be deleted if we do not work for a client for 12 months (no invoices issued). Once a client becomes non-active and the DPO confirms this, then the client folder should be archived by IT. Before archiving, all personal data and confidential information in the ‘0’ folder should be deleted from the folders. The IT team will do this at the time of archiving.
* You should follow the Archiving policy attached as Annex 2 to this policy document for all email boxes, calendars and platforms such as Teams and Zoom.
* If personal data is shared with faculty, translators or any third parties (as allowed by client contracts), we must receive written confirmation that the information has been deleted and destroyed once it is no longer needed. Faculty should confirm on a six-monthly basis that they hold no personal data or confidential information.

#### Issue Reporting

* Report any data requests or issues to the Data protection officer (currently Mark Abell) immediately
* Check with the Data Protection Officer if you are unsure about any aspect of storing, processing or sharing personal data.
* Think data protection in all planning and process
* You will find training resources at: shared/company docs/data protection and on Natural HR.
* If you come across any process or design idea that is not GDPR compliant (i.e., is ineffective in terms of data protection or does not put personal data protection front and centre of the plans), inform the Data Protection Officer.

## Data Protection Principles

The General Data Protection Regulation regulates how companies, including Imparta, must collect, handle and store personal data. These rules apply regardless of whether personal data is stored electronically, on paper or in any other way.

### 3.1 Article 5 of the GDPR requires that personal data shall be:

#### 3.1.1 Processed lawfully, fairly and transparently in relation to individuals.

This means we must have a legitimate reason for processing the data under the GDPR and be clear in all our communications about how data is to be used. Our legitimate grounds for processing are covered in the Section ‘Personal Data held by Imparta and Lawful Basis for Processing.’

#### 3.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This means we must not collect personal data for one purpose and then use it for another. If it becomes necessary to change the purpose for which an individual’s data is processed, the individual must be informed of the new purpose before any processing for that purpose occurs.

#### 3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This means we must only collect personal data to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

#### 3.1.4 Accurate and, where necessary, kept up to date.

This means we must take every reasonable step to ensure that personal data is accurate. It should be erased or rectified without delay where it is inaccurate or outdated. You must check the accuracy of any personal data at the point of collection and (subject to the following) at regular intervals afterwards.

However, do note that you may only make changes to:

* Customer Personal Data in accordance with instructions from the relevant data subject;
* Company Personal Data where you are authorised to do so in line with your role at Imparta; and
* Marketing Personal Data in accordance with instructions from the relevant data subject.

You will take due care in making any such changes and completing any audit log process that may be required.

#### 3.1.5 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.

This means we must not keep personal data longer than is necessary for the purpose or purposes for which they were collected and must take all reasonable steps to destroy or erase all data no longer required from our systems. To comply with this principle:

* + You must not collect any personal data from a data subject once the underlying agreement to do so has ended.
  + System Administrators will ensure (to the extent required by the GDPR, other applicable legislation, and contractual agreements with our customers) that personal data is removed from our online information systems that process or store personal data within 12 months from when the agreement under which it is processed has ended or at a later time if required to be kept longer by UK/EU legislation.
  + System Administrators will ensure that personal data is not retained in offline backup media for more than seven (7) years.

#### 3.1.6 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.

This means we must have effective security to protect personal data when receiving, storing, and transferring it. IT Security is covered in the Imparta policy document ‘IT Security,’ the policies in this document are mandatory for all staff.

Article 5 (2) of the GDPR requires that: ‘the Controller shall be responsible for, and be able to demonstrate, compliance with the principles.’

## Personal Data held by Imparta and Lawful Basis for Processing

### 4.2 The type of personal data that we collect and process in our business is as follows:

#### 4.2.1 Customer Personal Data

Customer Personal Data of our customers and their employees, including information on their performance (for example, training needs analysis, participation in online learning (for instance, on i-Coach, assessments and coaching reports), and personal contact information and any information identifying customer employees. In processing this data, we act as the Data Processor. The customer determines the nature, timing and purpose of the processing. The lawful basis for processing this data is in fulfilling our contractual obligations to our customers.

#### 4.2.2 Company Personal Data

Personal data on our employees, contractors, faculty and other associates. This data may include personal contact information, employment-related information such as salaries, benefits, performance reviews, disciplinary information, passport information, attendance records and other information required for the efficient running of the company. In processing this data, we act as the Data Controller. The lawful basis for processing is our legitimate interest in meeting our legal obligations to our staff and associates, our legitimate interest in running Imparta efficiently and effectively, and our communicating with staff and associates under all circumstances. We maintain a Legitimate Interest Assessment for these activities as a separate document that may be requested from the Data Protection Officer.

#### 4.2.3 Marketing Personal Data.

For example, names, addresses, email addresses and other contact details are collected from individuals who sign up for our newsletters or whose details we maintain on our contact sales and marketing mailing and data lists. In processing this data, we act as the Data Controller. The lawful basis for processing is that of Legitimate Interest. Our legitimate interest is in contacting clients and prospects about our services, events, research and other information and news. We maintain a Legitimate Interest Assessment for these activities as a separate document that may be requested from the Data Protection Officer.

The above personal data may include data we receive directly from a data subject (for example, directly from our employees and our customers, or more generally by individuals corresponding with us by mail, phone or email, as well as data we receive from other sources (including from our business partners, and sub-contractors in technical and payment services).

## Imparta as Data Controller and Data Processor, Definitions and Responsibilities

### 5.1 Controllers and Processors

#### 5.1.1 The GDPR applies to ‘Controllers’ and ‘Processors’:

The GDPR applies to ‘personal data,’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides a wide range of personal identifiers to constitute personal data, including name, identification number, email address, location data or online identifier, reflecting changes in technology and how organisations collect information about people. Companies that process, collect or store this data are known as Data Controllers or Data Processors.

A Data Controller determines the purposes and means of processing personal data.

A Data Processor is responsible for processing personal data on behalf of a Data Controller.

When we act as a Data Controller (in the case of Company Personal Data and Marketing Personal Data), this is because we are determining the purposes and means of processing the data, and the GDPR places specific legal obligations on us. These are summarised in Section 6 onwards.

Many people at Imparta will be more involved with working with Customer Personal Data. In processing this data, we act as the Data Processor as we are under the instructions of the client, who is the Data Controller. Although we act as a Data Processor, we must enable our clients, the Data Controllers, to meet their obligations under GDPR. This means we need to be aware of their Data Controller obligations and capable of helping them meet them. This means the difference in the roles is, in practice, limited (though the legal position is quite different), but the GDPR puts the following obligations on us as a Data Processor:

*Processing to meet the requirements of this Regulation*

Data Controllers may only appoint Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR. Processors are required to process personal data in accordance with the Data Controller's instructions. This is a broad brush and imposes an indirect obligation to comply with many of the requirements that apply to Controllers, albeit at their instruction. This also means we are obliged to follow the instructions of Data Controllers where they are legal and where we are reasonably able to do so.

*Restrictions on sub-contracting*

The GDPR gives Data Controllers a wide degree of control in terms of the ability of the processor to sub-contract. In effect, processors require prior written consent. This can be general, but even where general consent has been given, the Data Processor is still required to inform the Data Controller of any new sub-processors, giving the Controller time to object.

We use Microsoft Azure’s cloud services as a sub-processor for i-Coach. We will seek permission for this arrangement up front in all our client contracts. We cannot appoint any other third-party processor without the permission of all clients (Data Controllers) who will be impacted.

Salesforce is deployed for marketing, sales and finance data. When we use Salesforce, we act as the data controller, have all the responsibilities of the data controller, and must demonstrate a legal basis for the processing. This data is not subject to the Data Processor contracts we sign with our clients (see next paragraph).

*Controller/Processor contract*

A binding contract issued by the Data Controller must govern Data Processor activities. The binding obligations of the Data Processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Data Controller. There are several specific requirements, including that the personal data is processed only on documented instructions from the Data Controller and requirements to assist the Controller in complying with many of its obligations. The Data Processor has an obligation to tell the Controller if it believes an instruction to hand information to the d breaches the GDPR or any other EU or Member State law. This means we must always have a GDPR-compliant contract with any company whose personal data we handle.

*Demonstrating compliance*

One of the threads that runs through the GDPR is the requirement to demonstrate compliance. Processors are obligated to maintain a record of all categories of processing activities. This must include details of the Controllers and any other processors and of any relevant Data Protection Officers (DPOs), the categories of processing carried out, details of any transfers to third countries and a general description of technical and organisational security measures. These records must be provided to the supervisory authority on request. We comply with this through the record-keeping and audit trail provided by i-Coach.

*Security*

Processors, like Controllers, are required to implement appropriate security measures. Regular testing of the effectiveness of any security measures is also required where appropriate. We comply with this through a wide range of security measures – see Section 7.4 for details.

*Breach notification.*

We are required to notify Data Controllers and the Information Commissioners Office of any breach in data security. We comply with this through the provisions set out in Section 9 of this document.

*Data Protection Officers*

Data Controllers and Processors are required to appoint Data Protection Officers (DPOs) in certain situations, including in our case, where the data processing activities require regular monitoring of data subjects on a large scale. The DPO must have a degree of independence and is the contact point for any data subjects and the supervisory authority. The primary role of the DPO is to assist the processor with and advise on compliance with the GDPR. We have appointed Mark Abell as our DPO.

*Transfers to third countries*

While we are required to follow the relevant Data Controller's instructions with regard to the data processing, no matter what those instructions are, we can only transfer personal data to a third country (in the absence of an adequacy decision) if the Controller or Processor has provided appropriate safeguards and on condition that data subjects have enforceable rights in that country with respect to the data. This means that while we can transfer data within the EU and UK, we should not share data on EU and UK data subjects outside the EU and UK without the permission of the Data Controller and without being sure that the data subject’s rights are protected. This does not prevent us from sharing US personal data, for example, with US clients, but would stop us from transferring data on EU and UK subjects to a third country unless we have checked that sufficient regulation is in place. You must consult our DPO if you have any questions before you consider transferring personal data to any third country. Typically, data is downloaded from i-Coach directly by the client (Data Controller); this means that any data transfer from this point is the client’s responsibility.

## Individual Rights under the GDPR and How We Comply

As a Data Controller for our own Company's Personal Data and Marketing Personal Data, we must protect individual rights under the GDPR. As a Data Processor for Customer Personal Data, we must enable our clients (Data Controllers) to meet their obligations. Individual rights to control the use of their personal data are a core component of the GDPR and one of the main reasons the GDPR was enacted by EU and UK authorities.

The GDPR provides the following rights for individuals:

1. The Right to Be Informed
2. The Right of Access
3. The Right to Rectification
4. The Right to Erase
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights in Relation to Automated Decision Making and Profiling

### 6.1 The Right to Be Informed

#### 6.1.1 Overview

This right covers Imparta’s obligation to provide ‘fair processing information,’ typically through a privacy notice. It emphasises the need for transparency over how Imparta uses personal data. To comply with the GDPR, the information we supply must be concise, intelligible, easily accessible and free of charge.

#### 6.1.2. Imparta Policy

This table in Annex 1 outlines the information required in privacy policies and how Imparta should comply. Privacy policies will be maintained for i-Coach, the Imparta website, and marketing mailings.

### 6.2 The Right of Access

#### 6.2.1. Overview

This right allows individuals to access their personal data and be aware of and verify the lawfulness of the processing. Information must be provided within one month of receipt of a request. The provision of the information must be free of charge; however, if the requests are excessive or repetitive, fees can be charged.

#### 6.2.2. Imparta Policy

*When we are the Data Processor (Customer Personal Data)*

The request should come from the company’s Data Protection Officer or an individual authorised to make the request.

*When we are the Data Controller (Company Personal Data and Marketing Personal Data)*

Data subjects must make a formal request for information we hold about them, which must be made in writing. Employees who receive a written request should forward it to the Data Protection Officer immediately.

When receiving telephone enquiries, we must check the caller’s identity and suggest that the caller put their request in writing so that it can be dealt with as above. We must always verify the identity of anyone making a subject access request before handing over any information.

Requests for rectification should be passed to the Data Protection Officer. The Data Protection Officer will work with i-Coach and Salesforce administrators to locate, check, and, if necessary, correct the data. Copies must be easily readable.

The Data Protection Officer will keep a log of such enquiries and will ensure requirements for timeliness, accuracy and clarity are met.

### 6.3 The Right to Rectification

#### 6.3.1. Overview

The GDPR gives individuals the right to have personal data rectified where it is inaccurate or incomplete. Compliance has to be within one month of the request. This must also be rectified if inaccurate information has been passed to third parties.

#### 6.3.2. Imparta Policy

*When we are the data processor (Customer Personal Data)*

The request should come from the company’s Data Protection Officer or an individual authorised to make the request. The request should be in writing with the nature of their authorisation specified.

*When we are the data controller (Company Personal Data and Marketing Personal Data)*

Requests for rectification should be passed to the Data Protection Officer. The Data Protection Officer will work with i-Coach and Salesforce administrators to locate, check, and, if necessary, correct the data. The Data Protection Officer should inform the individual when this is complete.

The Data Protection Officer will keep a log of such enquiries and will ensure requirements for timeliness, accuracy and clarity are met.

### 6.4 The Right to Erasure

#### 6.4.1. Overview

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

#### 6.4.2. When does the Right to Erasure apply?

The Right to Erasure does not provide an absolute ‘right to be forgotten.’ Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

* 1. Where the personal data is no longer necessary about the purpose for which it was initially collected/processed.
  2. When the individual withdraws consent.
  3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  4. The personal data was unlawfully processed (i.e., otherwise in breach of the GDPR).
  5. The personal data must be erased to comply with a legal obligation.
  6. The personal data is processed in relation to the offer of information society services to a child.

As well as the individual’s right to request the erasure of their data, we also must consider:

* 1. The right of the Data Controller (our clients) to request the deletion of the records we hold on their behalf.
  2. The general principle that personal data should be held ‘no longer than is necessary.’

#### 6.4.3. Imparta Policy

*When we are the Data Processor (Customer Personal Data)*

The request should come from the client in written form and be passed to our DPO for recording and action.

1. If the client asks us to sign up to their data retention policy, this should be recorded by the Data Protection Officer and acted on by the relevant administrators.
2. The request should come from the company’s Data Protection Officer or an individual authorised to make the request. The request should be in writing with the nature of their authorisation specified. Erasure should occur as soon as practicable, but at least within one month.
3. If we have not invoiced a client for 12 months, finance should notify the Data Protection Officer. The Data Protection Officer will then speak to the Client Director responsible for the account, who will inform the account and ask whether there is any justifiable reason the data should be kept (for example, if the project may restart). If there is no justifiable reason or response, the data will be deleted within one month of the initial notification from Finance.
4. The Data Protection Officer should be informed if we know a client contract has ended and the data is no longer required. The Data Protection Officer will arrange for the deletion of all applicable data. The client will be informed that this data has been deleted.
5. Any backup tapes holding client data must be held offline and be encrypted to deny access. Backup tapes may not be loaded back onto servers until any data folders on the tapes have been deleted.

*When we are the Data Controller (Company Personal Data and Marketing Personal Data)*

If appropriate, Imparta will delete all data when requested to do so by individuals within one month of the request and will notify the individual or client when deletion is completed. Imparta reserves the right to hold the date for legitimate purposes and to meet legal requirements. If the request is from an individual, the request should be passed to the Data Protection Officer, who will assess the validity of the request and, if appropriate, work with the relevant platform administrators to locate and delete the data.

### 6.5 Right to Restrict Processing

#### 6.5.1 Overview

Individuals have a right to ‘block’ or suppress the processing of personal data.

When processing is restricted, you are permitted to store the personal data but not further process it.

You can retain just enough information about the individual to ensure that the restriction is respected in future.

#### 6.5.2 Imparta Policy

*When we are the data processor (Customer Personal Data)*

The request should come from the company’s Data Protection Officer or an individual authorised to make the request. The request should be in writing with the nature of their authorisation specified.

*When we are the Data Controller (Company Personal Data and Marketing Personal Data)*

If an individual asks us not to process their data, we will enforce this by deleting it in line with our Retention Policy. This is practical, as the limited use we make of data means there is no value for any party in us holding it if the limited uses are restricted. It also reduces the chance of future errors.

Requests for restriction of processing should be passed to the Data Protection Officer. The Data Protection Officer will work with i-Coach and Salesforce administrators to validate the request and locate, check, and delete the data. The Data Protection Officer should inform the individual when this is complete.

The Data Protection Officer will keep a log of such enquiries.

### 6.6 Right to Data Portability

#### 6.6.1 Overview

The Right to Data Portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another safely and securely, without hindrance to usability.

#### 6.6.2. Imparta Policy

It is unlikely that individuals will ask us to port their data to third parties. If clients ask, then this request should be passed to the DPO.

If asked, requests should go to the Data Protection Officer and then be managed with the relevant platform administrator, normally i-Coach.

### 6.7 Right to Object

#### 6.7.1. Overview

Individuals have the Right to Object to the following:

* processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
* direct marketing (including profiling); and
* processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on ‘grounds relating to his or her particular situation.’

Imparta must stop processing the personal data unless:

* we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or
* the processing is for establishing, exercising, or defending legal claims.

#### 6.7.2. Imparta Policy

*When we are the data processor (Customer Personal Data)*

The request should come from the company’s Data Protection Officer or an individual authorised to make the request. The request should be in writing with the nature of their authorisation specified.

*When we are the Data Controller (Company Personal Data and Marketing Personal Data)*

We must inform individuals of their Right to Object at the point of first communication’ and in our privacy notices.

This must be ‘explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.’

If you receive any objections of this kind, you should notify the Data Protection Officer immediately.

### 6.8 Rights Relating to Automated Decision-Making and Profiling

#### 6.8.1. Overview

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

#### 6.8.2. Imparta Policy

We must continually identify whether any of Imparta’s processing operations constitute automated decision-making. Currently, they do not. If this changes, we will need to update our procedures to deal with the requirements of the GDPR. The Data Protection Officer is required to monitor any changes to processing operations in relation to the automation of decision-making and profiling.

## Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR’s transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR’s emphasis elevates their significance.

Imparta is expected to put comprehensive but proportionate governance measures into place. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data.

Imparta will implement technical and organisational measures that ensure and demonstrate that we comply. These include internal data protection activities such as staff training, internal audits of processing, reviews of internal HR policies, penetration tests and proper documentation.

### 7.1 Contracts

All contracts with clients where we process their personal data require contracts signed with specific GDPR data clauses. The contract is essential so that both parties are aware of their responsibilities. Our contracts will also explain that we use a third-party processor – Microsoft Azure – to hold all the data we store in i-Coach. The contracts include information on:

* the subject matter and duration of the processing;
* the nature and purpose of the processing;
* the type of personal data and categories of data subject; and
* the obligations and rights of the Data Controller.

Client contracts have been developed to meet GDPR requirements. The Data Protection Officer can provide template contracts. If you are unsure which contract to use, please consult the Data Protection Officer.

### 7.2 Documentation

The GDPR contains explicit provisions about documenting our processing activities. Good documentation is regarded as central to GDPR compliance. We must maintain records on several aspects of data management, such as processing purposes, data sharing and retention. The Information Commissioner’s Office can ask for these records at any time. These records must be kept current and reflect our current processing activities.

We will maintain the following GDPR-related documentation and information, which can be found in our internal policy folders or by asking the Data Protection Officer:

* The name and contact details of our organisation (and, where applicable, of other Controllers, our representative and our Data Protection Officer). This information is in this document and on our privacy statements.
* The purposes of our processing. Recorded in this document.
* A description of the categories of individuals and categories of personal data. Recorded in this document.
* The categories of recipients of personal data. Recorded in this document.
* Retention schedules. Recorded in the GDPR Retention Policy Document.
* A description of our technical and organisational security measures. Recorded in the Information Security Document.
* The lawful basis for the processing. Recorded in this document and privacy statements.
* The legitimate interests for the processing. Recorded in this document and privacy statements.
* Individuals’ rights. Recorded in this document.
* The source of the personal data. Recorded in this document and privacy statements.
* Records of consent. Not relevant.
* Controller-processor contracts. Recorded in our standard contracts.
* The location of personal data. Recorded in this document and our standard contracts.
* Data Protection Legitimate Interests Assessment (LIA) reports. Held by the Data Protection Officer.
* Records of personal data breaches. Held by the Data Protection Officer.

### 7.3 Data Protection by Design and Default

Under the GDPR, Imparta must implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. This is known as privacy by design.

This means that if we are designing or changing any product or service that involves the processing of data, then data protection should be integral to the design specifications.

The Executive and Management teams know this obligation and will ensure we comply. However, if you know any new, existing or amended products and services where you feel data risks have not been considered, you should speak to the Data Protection Officer.

### 7.4 IT and Data Security

IT and Data Security will always be a core activity for our IT and Software Development teams. All staff will be given IT and Data Security policies on arrival and will be trained on IT and Data Security on arrival and thereafter. If Staff are concerned they have received insufficient training, they should notify their manager immediately, and training will be arranged. IT and Data Security is maintained through an extensive range of activities and protocols, including:

* Physical Access Controls: To prevent unauthorised access, including security locks and passcodes on server rooms, office security, visitor controls, and CCTV on office entry.
* Availability controls: These include regularly checked fire systems and disaster recovery policies.
* IT security controls, including firewalls and up-to-date virus prevention software.
* Resilience and Capacity: Customer Personal Data is stored on i-Coach and hosted on the cloud-based Microsoft Azure platform. SharePoint drives and OneDrive is regularly backed up on Azure and can be accessed in an emergency. This ensures resilience, capacity, and flexibility and allows real-time management of processing power and data storage capacity
* Transmission Control: Password security and encryption, use of secure password-protected Azure-based collaboration services.
* Employee System Access Control: Only authorised employees have access to databases. Access must be audited and controlled with individual and uniquely identifiable access codes.
* Security Testing: Annual Penetration on all Imparta platforms testing with any risks above low status addressed immediately.
* Encryption: Customer Data is encrypted within Azure databases.
* VPN – all staff and faculty must use Imparta VPN in public spaces to protect data.

The software development team are the only employees with access to i-Coach and the database hosted on Microsoft Azure. The policies regarding the security management of this team relating to access to data are as follows:

* There must be defined user profile roles within the Development team. The software development team lead has administrator rights in Microsoft Azure to create and maintain the access of development users. The team leader will decide and record which team members have access to read, write, or alter data and extract backups of data.
* All development team members must be restricted from keeping users' personal data from the system on their local machines.
* Personal data is to be stored only in a Microsoft Azure SQL database in the cloud that is encrypted at rest. While developing on local machines, the software development team must only ever get an anonymised copy of the database.   
    
  - Development team activities to be tracked with tools within Microsoft Azure and Microsoft Azure DevOps.

## Storage and Transmission of Personal Data

### 8.1 Storage

This section describes how and where personal data should be safely stored. Questions about storing personal data can be directed to the Head of Information Technology or the Data Protection Officer.

Customer Personal Data will principally be stored on the Microsoft cloud-based Azure platform through i-Coach and our Microsoft 365 office environment. i-Coach and Windows 365 are hosted on the Microsoft Azure platform and deploy the Azure database functionality. Customer Personal Data on Azure is protected to the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018 and is therefore in line with the highest standards. See further details at: <https://azure.microsoft.com/en-gb/support/trust-center/>.

Data Controllers will ask for Customer Personal Data to be analysed, organised and shared in such a way that requires data sets to be downloaded from Azure. Imparta employees will also need to work on data samples to enable them to serve their clients. For example, a client may ask for data on workshop delegates over the last six months, which must be downloaded and shared.

Where personal data is not held in Microsoft 365 in the client folders, personal data should be kept in the ‘0’ Confidential folder in the client folder. This folder will have access security limiting access to the client team. Storing data here will also make deletion straightforward in line with the retention policy. Personal data may not be held or transferred to any devices that are not owned and subject to Imparta’s IT and Security policies. See Section 7.4 for more information on IT security.

Company Personal Data will also be held in our Salesforce (including Sage Financial plug-ins), HR Natural HR system, and on secure internal servers,

Marketing Personal Data will be stored on the cloud-based Salesforce CRM system and within the Hubspot CRM.

Our policy on the Azure platform is to keep all information within the EU or UK unless specifically required by the Data Controller to transfer it.

The administrative setup of Microsoft Azure will allow administrators to upload information either in the EU/UK or the USA. The ability to upload data to other locations will be removed. If a client requires data to be kept in a different location, then a separate database will be needed with similar restrictions for that location. Administrators must not, under any circumstances, circumvent this policy.

Customers can download personal information from i-Coach, but Imparta employees may only do so at a customer's request and when authorised.

Customer Personal Data must not be stored on internal company drives, folders, laptops, USB sticks or any other device or storage platform. Customers' personal data must not be stored on paper. Data printouts should be shredded immediately after usage.

Company personal data is kept securely by the HR department on Azure or in the Natural HR service.

Marketing personal data is only stored and managed on the Salesforce CRM (incorporating Pardot plug-in) system.

### 8.2 Safe Use and Transmission of Personal Data

When personal data is accessed and used, it is at the most significant risk of loss, corruption or theft. To limit this risk, you must:

* 1. when working with personal data, ensure the screens of your computer are locked or that you log off when they are unattended;
  2. not share personal data informally. In particular, you should never send personal data by email unless the data is in a document that is securely encrypted;
  3. if you are transmitting personal data to customers (having been downloaded from i-Coach (as described above), then the transmission must be through a secure, shared site such as Microsoft Teams or your client’s secured collaboration service (such as Cisco’s’ Box service) or a password-protected document sent by email.
  4. Use the integrated rights management system in Microsoft Teams for added security.
  5. Personal data may not be held or transferred to any devices that are not owned and subject to Imparta’s IT and Security policies. See Section 7.4 for more information on IT security.
  6. All mobile phones with Imparta applications (for example, Imparta email, SharePoint, Salesforce, Teams) on them must have 6-figure passwords.
  7. All Imparta staff must use Imparta’s private VPN when working in public areas.

### 8.3 Administrative Access to Databases Holding Personal Data

Only those authorised to do so will have direct access to the Azure database. Authorisation to access databases may only be given by the Data Protection Officer and Head of Software Development. All those with authorisation will be required to use multi-factor data authentication. Within the Azure environment, administrators will only be given access to the assets and data they need and are authorised to have. For example, IT systems administrators will not need access to i-Coach databases.

## Incident Reporting

If you become aware or suspect that personal data has been:

1. passed to a third party without permission;
2. lost or stolen;
3. corrupted or maliciously altered;
4. accessed illegally online or in any other form or
5. processed, used or treated in any way that is not compliant with this Policy;

Then, you should immediately report the incident to the Executive Team Member responsible for your area. The Executive Team Member should then inform the Data Protection Officer and the CEO, and a plan will be determined to reduce and mitigate the event's impact. If the personal data in question is Customer Personal Data, then a Director of the Company will inform and consult with the customer in line with the agreements in place with the Customer.

The GDPR requires us to report certain types of personal data breaches to the relevant supervisory authority (in our case, the Information Commissioners Office). We must do this within 72 hours of becoming aware of the breach.

If the breach is likely to result in a substantial risk of adversely affecting individuals’ rights and freedoms, we must also inform those individuals without undue delay.

The Data Protection Officer will keep a record of any personal data breaches, regardless of whether we must notify the concerned individuals.

## Access to, and Disclosure and Transfer of, Personal Data

### 10.1 Access to Personal Data

Our Information Technology team will ensure that access to personal data is granted at a reasonable level of granularity only as is necessary for a worker to perform their role. Anonymous personal data should be used where possible. The practice of least privilege access should apply.

### 10.2 Sharing Personal Data

Personal data must not be shared with other workers unless the recipient has been granted access to the same source of personal data or has a clear need to access that level of personal data.

We can only share personal data with selected third parties for the purposes data subjects are informed of. Therefore:

* you should only share personal data with customers or customer employees as required to perform the services being provided to the customer by Imparta and
* you should not share any personal data with other third parties without first getting permission from the Data Protection Officer.

### 10.3 Transferring Personal Data Outside of the EEA

Personal data created within the European Economic Area (‘EEA’) may be circulated within the EEA (provided that such data has been collected lawfully and is being processed fairly and lawfully and in accordance with the data subject’s rights under GDPR).

The GDPR restricts us from transferring any personal data we hold to any location outside the EEA unless one of the following conditions applies:

* the country to which the personal data are transferred ensures an adequate level of protection for the data subject’s rights and freedoms;
* the data subject has given consent;
* the transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the data subject or to protect the vital interests of the data subject;
* the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims or
* The transfer is authorised by the relevant data protection authority, where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to those requirements above, personal data we hold may be accessed by staff operating outside the EEA who work for us or for one of our clients but only with the permission of the client (Data Controller) or owner of the data.

You must not transfer personal data to any party where the receiving party is located outside of the EEA without seeking assistance from the Data Protection Officer.

### 10.4 Disclosing Data for Other Reasons

In certain circumstances, the GDPR allows us to disclose personal data to law enforcement agencies without the data subject's consent.

Under these circumstances, Imparta may decide to disclose the requested personal data. However, before doing so, we must ensure the request is legitimate and give it adequate consideration, seeking assistance from the Board and our legal advisors where necessary.

If you are contacted by any law enforcement agency (or anyone other than the data subject of the personal data in question) requesting its disclosure, you should forward the request to your line manager or the Data Protection Officer immediately.

## Compliance and Updates

Imparta reserves the right to change this Policy at any time. Where appropriate, we will notify data users of those changes by mail or email.

## Annex 1: Privacy Policy Contents

The table below lists the information that must be included and updated in our privacy policies.

|  |  |  |  |
| --- | --- | --- | --- |
| **What information must be supplied in Imparta’s privacy notices?** | | **Data obtained directly from the data subject** | **Data not obtained directly from the data subject** |
| Purpose of the processing and the lawful basis for the processing.  Data may be processed to implement and organise training events (i-Coach).  Data may be processed to implement skills and competency assessments (i-Coach).  Data may be processed for marketing purposes (Salesforce). | | ✓ | ✓ |
| The legitimate interests of the Controller or third party, where applicable. | | ✓ | ✓ |
| Categories of personal data. | |  | ✓ |
| Any recipient or categories of recipients of the personal data.  Imparta and our clients will be the only recipients of this information. | | ✓ | ✓ |
| Details of transfers to third country and safeguards.  All information is to be held in Europe. | | ✓ | ✓ |
| Retention period or criteria used to determine the retention period.  Data is to be retained only as long as it is needed. | | ✓ | ✓ |
| The existence of each of the data subject’s rights. | | ✓ | ✓ |
| The right to withdraw consent at any time, where relevant. | | ✓ | ✓ |
| The right to lodge a complaint with a supervisory authority.  Details of the supervisory authority of the Information Commissioner’s Office are to be included. | | ✓ | ✓ |
| The source the personal data originates from and whether it came from publicly accessible sources.  Information on i-Coach will come from clients/data subject’s employers.  Information in SharePoint will come from opt-in or publicly available sources. | |  | ✓ |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.  Not applicable. | | ✓ |  |
| The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences.  Imparta does not carry out automated decision-making. | | ✓ | ✓ |
| When should information be provided? | At the time the data are obtained. | Within a reasonable period of having obtained the data (within one month) | |
| If the data are used to communicate with the individual, at the latest, when the first communication takes place; or | |
| If disclosure to another recipient is envisaged, at the latest, before the data are disclosed. | |

## Annex 2: Archiving Policy

## Client Services (CS) mailbox

The Client Services Mailbox is used for incoming requests from clients and Imparta colleagues about workshops and other services we deliver.

All client emails regarding clients that no longer work with us are to be moved to the 4, Dormant Clients subfolder in the CS mailbox. This subfolder will be emptied once every six months by the IT team.

Once every six months, Mark Abell will inform the Delivery and Operations Team Lead and PM team lead which clients no longer work with us.

Any files, documents, or materials that need to be kept should be kept in the Q drive and not stored in the mailbox. Once personal data has been transferred to the Q drive, it can be deleted from the mailbox.

The FDM should review their folders and subfolders every quarter.

The Delivery and Operations Team Lead manages this process.

## Client mailbox calendars

Client Mailbox Calendars are used to share training event information with clients.

If you set up a client mailbox calendar, you should only allow access to those needing it. Access permissions should be checked regularly, and for those who no longer require, access is removed.

The client calendar must be deleted if we cease working with a client. Once every six months, Mark Abell will inform the Delivery and Operations Team Lead and PM team lead what clients no longer work with us.

The Delivery and Operations Team Lead manages this process.

## MS Teams membership

MS Teams is used to share documents and have conversations with clients. Most clients have a Team allocated to them.

Only people active on an account should be on a Team. People who have left the project or company, on either the Imparta or client sides, should be removed.

Faculty are not Imparta employees and should not have access to personal data or confidential information unless they have specific permission to do so (check with Mark Abell). If Faculty are involved in a Team, they should be in a secure channel where they only see, and have access to, the personal data and information they need.

All MS Teams need to be checked regularly by Team owners for the presence of Faculty members and participants who should no longer be there. Old client accounts where we no longer work with the client should be deleted.

Keeping Teams organised and correct is the responsibility of each Team owner. Managers of Team owners should check with their team members that their Teams are correct at least quarterly.

Recordings on Teams should only be kept as long as necessary. Recordings will be automatically deleted after 180 days. If you need to keep these recordings, move them to the ‘0’ confidential folder in the appropriate client folder.

## Q-drive

The Q Drive is the home of all documents relating to client projects.

Any personal data or client confidential information MUST go in the 0. Confidential folder within the Client folder. If there is any of this data in other subfolders of the Client Workshare, this needs to be moved into 0 or removed entirely.

A screenshot of a computer

Description automatically generated

Managers are to verify the Client Work folders regularly to ensure no confidential data is present. IT will scan for XL files that are not in the O folder and check for personal data being kept incorrectly.

Every three months, Monika will be going through the Client Work folder to check whether the clients are still live. If not, these folders will be archived, and the 0 folders will be removed.

## i-Coach Zendesk mailbox

The i-Coach Zendesk mailbox is used to correspond and monitor responses to help requests from users of i-Coach.

The Zendesk account should only have active requests held; all legacy requests should be deleted.

Registered accounts, which are accounts set up by i-Coach users to interact with Zendesk, should be deleted by the Digital Participant Manager once they are 12 months old. This process should be diarised to take place once a quarter.

The Digital Participant Manager manages this.

## i-Coach Support mailbox

The i-Coach support mailbox receives client requests relating to i-Coach and deals with i-Coach issues. The Digital Participant Manager manages it.

Emails older than 12 months are to be deleted, but ideally, completed emails should be deleted on an ongoing basis.

The Digital Participant Manager manages this.

## Local folders

All staff should regularly empty their Downloads, Desktop, and Documents folders on their local computer. These are not secure places to store data or confidential information.

## Zoom recordings

Monthly checks on the requirement of recordings present in your own Zoom account. Nothing over three months is to be kept unless essential.

Zoom has now been set to automatically delete recordings older than 180 days. If you need to keep these recordings, move them to the ‘0’ confidential folder in the appropriate client folder.

## Imparta personal mailbox

Personal data and confidential information should not be stored in your Imparta’s personal email mailbox. Any attached items, including these types of data, should be saved in the correct place, typically the client folder ‘0’ folder. The attachment can then be deleted from the email. Should the body of the email also have personal data or confidential information involved within the email itself, it should also be saved to the correct location and deleted from the mailbox.

RETENTION

i-Coach backups are retained for six months and are then deleted. SharePoint backups are deleted after 12 months.