PSYTECH DATA PROTECTION POLICY

V1.1

PSYTECH Data Protection Policy

1 Introduction

1.1 Purpose

The goal of this policy is to codify PSYTECH's commitment to protecting the rights and freedoms of data subjects, safely and securely processing their data in accordance with legal obligations.

PSYTECH holds personal data about assessment participants, clients, and distributors for the overarching primary purpose of executing, scoring, and reporting on the outcome of psychometric assessments and other questionnaires or surveys.

This policy defines how PSYTECH aims to protect personal data and ensure that its staff understands the rules governing the use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Managing Director - in his or her role as Data Protection Officer - be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.2 Version

Version	Date	Owner
1.1	1 September 2019	Managing Director

1.3 Control of Hard-Copy Versions

The digital version of this document residing in PSYTECH's document repository should be considered the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. Any printed version of this manual is uncontrolled and should therefore be considered unreliable.

1.4 Related Documents

The PSYTECH Data Protection Policy governs the *PSYTECH Privacy Policy*.

1.5 Definitions

Business purposes	The purposes for which personal data may be used by PSYTECH (the *Data Processor*) and its clients (the *Data Controllers*) are: • Inviting people to online psychometric assessments, surveys, and other questionnaires. • Collecting biodata to be used in aggregated statistical analysis of assessment data. • Collecting responses from psychometric assessments, surveys, and other questionnaires • Producing individual and group reports from psychometric assessments, surveys, and other questionnaires. • Tracking and reporting on assessment progress. • Analysing data from psychometrics assessments, surveys, and other questionnaires for the purpose of assessment development and assessment validation. • Complying with legal, regulatory and corporate governance obligations and good practice. • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests. • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, • Investigating service issues, security incidents, and complaints. • Improving services.

	Personal data may be used by PSYTECH's clients (the *Data Controllers*) for additional reasons such as personnel selection and identifying development needs, and as the *Data Controllers* it is their responsibility to define these purposes and disclose them to their end users.
Personal Data	Personal Data means any information relating to an identified or identifiable natural person (*Data Subject*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data that PSYTECH gathers primarily includes individuals' names, email addresses, and sex. It may also include biographical data such as ethnicity, educational, and occupational data, plus other relevant data required by PSYTECH's clients (the *Data Controllers*).
Special Categories of Personal Data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information. Any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data Controller	*Data Controller* means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the end purposes of the processing of personal data; where the purposes and means of such processing are determined by law.
Data Processor	*Data Processor* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	*Processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for PSYTECH depends on the jurisdiction under which data protection is governed, and may include: • Albania: Information and Data Protection Commissioner (IDP) (Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (KDIMDP)) • Andorra: Data Protection Agency of Andorra (Catalan: Agència Andorrana de Protecció de Dades (APDA))

	• Australia: Office of the Australian Information Commissioner • Austria: Austrian Data Protection Authority (German: Datenschutzbehörde) • Belgium: Commission for the Protection of Privacy (Dutch: Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), French: Commission de la protection de la vie privée (CPVP)), also known as CPP • Brazil: National Data Protection Authority (ANPD)[3] • Bulgaria: Bulgarian Data Protection Authority • Canada: Office of the Privacy Commissioner of Canada • Croatia: Croatian Personal Data Protection Agency (Croatian: Agencija za zaštitu osobnih podataka (AZOP)) • Cyprus: Office of the Commissioner for Personal Data Protection • Czech Republic: Office for Personal Data Protection (Czech: Úrad pro ochranu osobních údaju (ÚOOÚ)) • Denmark: Danish Data Protection Agency (Danish: Datatilsynet) • Estonia: Estonian Data Protection Inspectorate (Estonian: Andmekaitse Inspektsioon) • Finland: Office of the Data Protection Ombudsman (Finnish: Tietosuojavaltuutetun toimisto) • France: Commission nationale de l'informatique et des libertés (lit. 'National Commission on Informatics and Liberty'), also known as CNIL • Germany: Federal Commissioner for Data Protection and Freedom of Information (German: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)) • Greece: Hellenic Data Protection Authority, also known as HDPA • Guernsey Guernsey: Data Protection Office • Hungary: Hungarian National Authority for Data Protection and Freedom of Information (Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)) • Iceland: Data Protection Authority (Icelandic: Persónuvernd) • Ireland: Data Protection Commissioner (Irish: An Coimisinéir Cosanta Sonraí), also known as DPC • Isle of Man: Office of the Data Protection Supervisor • Israel: The Privacy Protection Authority • Italy: Italian Data Protection Authority (Italian: Garante per la Protezione dei Dati Personali), also known as Italian DPA • Latvia: Data State Inspectorate (Latvian: Datu valsts inspekcija) • Liechtenstein: Datenschutzstelle • Lithuania: State Data Protection Inspectorate (Lithuanian: Valstybine duomenu apsaugos inspekcija (VDAI)) • Luxembourg: National Commission for Data Protection (German: Nationale Kommission für den Datenschutz, French: Commission nationale pour la protection des données), also known as CNPD • Malta: Office of the Information and Data Protection Commissioner, also known as IDPC

	• Mexico: National Institute of Transparency for Access to Information and Personal Data Protection (Spanish: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)) • Monaco: Commission de contrôle des informations nominatives (lit. 'Personal Data Control Board'), also known as CCIN • Morocco: Commission nationale de contrôle de la protection des données à caractère personnel (lit. 'National Commission for the Control of the Protection of Personal Data'), also known as CNDP • Netherlands: Dutch Data Protection Authority (Dutch: Autoriteit Persoonsgegevens (AP)) • New Zealand: Office of the New Zealand Privacy Commissioner • Norway: Norwegian Data Protection Authority (Norwegian: Datatilsynet) • Philippines: National Privacy Commission • Poland: Personal Data Protection Office (Polish: Urzad Ochrony Danych Osobowych (UODO)) • Portugal: National Commission Data Protection (Portuguese: Comissão Nacional de Proteção de Dados (CNPD)), also known as NCDP • Republic of Macedonia Macedonia: Directorate for Personal Data Protection • Romania: National Authority for the Supervision of Personal Data Processing (Romanian: Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal), also known as ANSPDCP • Russia: Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor) • Serbia: Commissioner for Information of Public Importance and Personal Data Protection • Slovakia: Office for Personal Data Protection of the Slovak Republic (Slovak: Úrad na ochranu osobných údajov Slovenskej republiky) • Slovenia: Information Commissioner of the Republic of Slovenia (Slovene: Republika Slovenija Informacijski pooblaščenec) • Spain - Andalusia: Transparency and Data Protection Council of Andalusia (Spanish: Consejo de Transparencia y Protección de Datos de Andalucía) • Spain - Basque Country: Basque Data Protection Authority (Basque: Datuak Babesteko Euskal Bulegoa, Spanish: Agencia Vasca de Protección de Datos) • Spain - Catalonia: Catalan Data Protection Authority (Catalan: Autoritat Catalana de Protecció de Dades (APDCAT)) • Spain: Spanish Data Protection Agency (Spanish: Agencia Española de Protección de Datos (AEPD)) • Sweden: Swedish Data Protection Authority (Swedish: Datainspektionen), also known as Swedish DPA • Switzerland: Federal Data Protection and Information Commissioner (German: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

	(EDÖB), French: Préposé fédéral à la protection des données et à la transparence (PFPDT), Italian: Incaricato federale della protezione dei dati e della trasparenza (IFPDT)), also known as FDPIC • United Kingdom: Information Commissioner's Office, also known as ICO • USA: No single national authority.

1.6 Scope

This policy applies to all PSYTECH staff, who must be familiar with this policy and comply with its terms.

This policy supplements PSYTECH's other policies pertaining to information security, particularly those governed by the *PSYTECH ISMS Information Security Policy*. PSYTECH may supplement or amend the *PSYTECH Data Protection Policy* with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

1.7 Control of Hard-Copy Versions

The digital version of this document residing in the document repository should be considered the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. Any printed version of this manual is uncontrolled and cannot be relied upon.

1.8 Terms and Definitions

- "We" and "Our" refer to PSYTECH as an organisational unit.

1.9 Responsibility

The Managing Director assumes the role of the Data Protection Officer (DPO) and has overall responsibility for the day-to-day implementation of the *PSYTECH Data Protection Policy*.

The Head Developer is responsible for implementing this policy in the context of PSYTECH infrastructure and software development practices.

2 Data Protection Principles

PSYTECH will comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. PSYTECH will make every effort possible in everything we do to comply with these principles.

2.1 GDPR Principles

2.1.1 Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2.1.2 Limited for its purpose

Data can only be collected for a specific purpose.

2.1.3 Data minimisation

Any data collected must be necessary and not excessive for its purpose.

2.1.4 Accurate

The data we hold must be accurate and kept up to date.

2.1.5 Retention

We cannot store data longer than necessary for the purposes for which it is used.

2.1.6 Integrity and confidentiality

The data we hold must be kept safe and secure.

2.2 Accountability and transparency

PSYTECH must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. PSYTECH is responsible for keeping a written records of how all the data processing activities it is responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, PSYTECH must demonstrate compliance. PSYTECH staff are responsible for understanding their particular responsibilities to ensure that PSYTECH meets the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conduct Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Anonymisation where applicable
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

3 Procedures

3.1 Fair and lawful processing

PSYTECH must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that PSYTECH should not process personal data unless the individual whose details we are processing has consented to this happening.

If PSYTECH cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

3.2 Controlling vs. processing data

PSYTECH is classified as a *Data Processor*. As a *Data Processor*, we must comply with our contractual obligations and act only on the instructions of the *Data Controller*. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

3.3 Lawful basis for processing data

PSYTECH must establish a lawful basis for processing data. PSYTECH must ensure that any data it is responsible for managing has a written lawful basis approved by the DPO. PSYTECH staff members are responsible for checking the lawful basis for any data they are working with and ensure that all of their actions comply the lawful basis. At least one of the following conditions must apply whenever PSYTECH processes personal data:

3.3.1 Consent

We have obtained recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

3.3.2 Contract

The processing is necessary to fulfil or prepare a contract for the individual.

3.3.3 Legal obligation

We have a legal obligation to process the data (excluding a contract).

3.3.4 Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

3.3.5 Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

3.3.6 Legitimate interest

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

3.4 Deciding which condition to rely on

If a PSYTECH staff member is making an assessment of the lawful basis, they must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. A lawful basis cannot be relied upon if it is reasonable to achieve the same purpose by some other means.

Remember that more than one basis may apply. PSYTECH staff members should rely on what will best fit the purpose, not what is easiest.

PSYTECH staff members should consider the following questions:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Am I in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Am I able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

PSYTECH must also ensure that individuals whose data are being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice, as per the *PSYTECH Privacy Policy*. This applies whether we have collected the data directly from the individual, or from another source.

If a PSYTECH staff member is responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, they must have this approved by the DPO.

4 Special Categories of Personal Data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where PSYTECH processes special categories of personal data, PSYTECH will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If PSYTECH does not have a lawful basis for processing special categories of data that processing activity must cease.

5 Responsibilities

5.1 PSYTECH's responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identifying the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report, and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised

5.2 Responsibilities of all PSYTECH staff members

- Fully understand your data protection obligations

- Check that any data processing activities you are dealing with comply with PSYTECH's policies and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it, or otherwise cause PSYTECH to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

5.3 Responsibilities of the Data Protection Officer

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

5.4 Responsibilities of the Head Developer

- Ensuring that all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

5.5 Responsibilities of the Communications Director

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

5.6 Accuracy and relevance

PSYTECH will ensure that any personal data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. PSYTECH will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If a PSYTECH staff member believes that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the DPO.

5.7 Data security

PSYTECH must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

5.8 Storing data securely

All data storage should comply with the *PSYTECH ISMS Information Security Policy* and the sub-policies that it governs.

5.9 Data retention

PSYTECH must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

5.10 Transferring data internationally

There are restrictions on international transfers of personal data. PSYTECH staff must avoid transferring personal data abroad, or anywhere else outside of normal rules and procedures.

6 Rights of Individuals

Individuals have rights to their data which PSYTECH must respect and comply with to the best of our ability. PSYTECH must ensure individuals can exercise their rights in the following ways:

6.1 Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

6.2 Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

6.3 Right to rectification

- PSYTECH must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

6.4 Right to erasure

- PSYTECH must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

6.5 Right to restrict processing

- PSYTECH must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- PSYTECH is permitted to store personal data if it has been restricted, but not process it further. PSYTECH must retain enough data to ensure the right to restriction is respected in the future.

6.6 Right to data portability

- PSYTECH must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- PSYTECH must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

6.7 Right to object

- PSYTECH must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- PSYTECH must respect the right of an individual to object to direct marketing, including profiling.
- PSYTECH must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

6.8 Rights in relation to automated decision making and profiling

- PSYTECH must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

7 Privacy Notices

7.1 When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

7.2 What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- The purpose of processing the data
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- Detailed information of any transfers to third countries and safeguards in place
- The right to lodge a complaint

8 Subject Access Requests

8.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

8.2 How PSYTECH deals with subject access requests

PSYTECH must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt. PSYTECH endeavours to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. PSYTECH must obtain approval from the DPO before extending the deadline.

PSYTECH can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, PSYTECH can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, PSYTECH must not change or amend any of the data that has been requested. Doing so is a criminal offence.

8.3 Data portability requests

PSYTECH must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a JSON file, although other formats are acceptable. PSYTECH must provide these data either to the individual who has requested it, or to the *Data Controller* they have

requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and permission must be obtained from the DPO first.

9 Right to Erasure

9.1 What is the right to erasure?

- Individuals have a right to have their data erased and for processing to cease in the following circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

9.2 How PSYTECH deals with the right to erasure

PSYTECH can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, PSYTECH must inform them of those recipients.

9.3 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. PSYTECH must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

PSYTECH must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

9.4 The right to restrict automated profiling or decision making

PSYTECH may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, PSYTECH must:

- Provide individuals with information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure that PSYTECH's systems are working as intended.

10 Third Parties

10.1 Using third party controllers and processors

As a *Data Processor*, PSYTECH aims to have written contracts in place with any third party *Data Controllers* and *Data Processors* that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a *Data Processor*, we must only act on the instructions or agreement of a *Data Controller*. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

We must only appoint other *Data Processors* who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

10.2 Contracts

PSYTECH's contracts aim to comply with any standards set out by the relevant *Supervisory Authority* and, where possible, follow standard contractual clauses which are available. Our contracts with *Data Controllers* and *Data Processors* should set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the *Data Controller*.

PSYTECH's contracts should include terms that specify:

- Acting only on written instructions or other relevant agreement
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the *Data Controller* and under a written contract

- The *Data Controller* will assist the *Data Processor* in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The *Data Processor* will assist the *Data Controller* in meeting its GDPR obligations in relation to the security of processing, notification of data breaches, and implementation of Data Protection Impact Assessments
- Submit to requested audits and inspections, and provide whatever information necessary for the *Data Controller* and *Data Processor* to meet their legal obligations.
- Nothing will be done by either the *Data Controller* or *Data Processor* to infringe GDPR.

11 Audits, Monitoring, and Training

11.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

11.2 Monitoring

All PSYTECH staff must observe the *PSYTECH Data Protection Policy*. The DPO has overall responsibility for this policy. PSYTECH will keep this policy under review and amend or change it as required.
PSYTECH staff must notify the DPO of any breaches of this policy. PSYTECH staff must comply with this policy fully and at all times.

11.3 Training

PSYTECH staff will receive adequate training on GDPR and provisions of data protection law specific for their role. PSYTECH staff must complete all training as requested. If staff move role or responsibilities, they are responsible for requesting new data protection training relevant to their new role or responsibilities. Staff requiring additional training on data protection matters should contact the DPO.

11.4 Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as staff have become aware of a breach. PSYTECH has an obligation to report any data breaches to the relevant *Supervisory Authority* in a timely fashion.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows PSYTECH to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the relevant *Supervisory Authority* of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures, will be liable to disciplinary action.

11.5 Failure to comply

PSYTECH takes compliance with this policy very seriously. Failure to comply puts both staff and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under PSYTECH procedures. This may result in dismissal. Any staff member with questions or concerns about anything in this policy should not hesitate to contact the DPO.