Physis

Data Protection Policy

Policy & Version:	Data Protection Policy V3
Author:	J Milton
Approved by:	M Johnson
Effective from:	10/04/2025
Last Reviewed	20/10/2026
Next Review	10/04/2027

Physis Quantum Limited
1 Marlowe Court, Shakespeare Way, Whitchurch, Shropshire, SY13

Data Protection Policy

CONTENTS

1. Overview, Policy Scope and Data Protection Principles
2. How we define personal data
3. Lawfulness, fairness & transparency
4. Consent
5. Transparency – notifying Data Subjects
6. Purpose limitations
7. Data minimisation
8. Accuracy
9. Storage Limitations
10. Security Integrity & confidentiality
11. How we define special categories of personal data
12. How we define processing
13. How we will process your personal data
14. Examples of when we might process your personal data
15. Retention of personal data
16. Sharing your personal data
17. Reporting a Personal Data Breach
18. Transfer limitations
19. How should you process personal data for the company?
20. How to deal with data breaches
21. Subject Access Requests (SARs)
22. Your data subject rights
23. Accountability
24. Record Keeping
25. Training and audit
26. Privacy by design and Data Protection Impact Assessment (DPIA)
27. Automated Processing and Automated Decision-Making
28. Direct Marketing
29. Sharing personal data
30. Changes to this Data Protection Policy

Appendix 1 – Data Consent Form

DATA PROTECTION POLICY

for Employees, Workers and Consultants

Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **UK General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, directors, apprentices and consultants, however the Company also hold data for our service users, their families, and third parties such as suppliers. Anyone who falls into one of these categories, are considered a **'data subject'** for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, services users, clients or supplier contacts, shareholders, website users or any other data subject.

1.4 The Company has measures in place to protect the security of your data in accordance with our Data Security provider.

1.5 The company will hold data in accordance with our Data Retention requirements. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.8 This policy does not form part of your contract with the Company and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

1.9 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

1.10 This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

Scope of policy and when to seek advice on data protection compliance

1.11 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

1.12 All Directors, individual business areas, departments, line managers, and employees are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

1.13 The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Mel Johnson, and they can be reached at 07772 966032 and mel@physisgroup.co.uk.

1.14 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Company);
- if you need to rely on Consent or need to capture Explicit Consent;
- if you need to draft Privacy Notices;
- if you are unsure about the retention period for the Personal Data being Processed;
- if you are unsure what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data Breach;
- if you are unsure on what basis to transfer Personal Data outside the UK;
- if you need any assistance dealing with any rights invoked by a Data Subject;
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than for which it was collected;
- if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
- if you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

Data Protection Principles

1.15 Personal data must be processed in accordance with the '**Data Protection Principles**.' It must be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- accurate and where necessary kept up to date (Accuracy);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are accountable for these principles and must be able to show that we are compliant.

2 How we define personal data

2.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

2.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

2.3 The personal data might be provided to us by you, or someone else (such as a former employee, doctor or health professional or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of a contract of employment (or services) or after its termination. It could be created by your manager or by your colleagues.

2.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to criminal convictions as disclosed by DBS and your suitability to work with children;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

3 Lawfulness, fairness and transparency

3.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

3.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

3.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given their Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

3.4 You must identify and document the legal ground being relied on for each Processing activity.

4 Consent

4.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

4.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

4.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

4.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

4.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines, so that the Company can demonstrate compliance with Consent requirements.

5 Transparency (notifying Data Subjects)

5.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of

the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

5.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

5.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

6 Purpose limitation

6.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

6.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

7 Data minimisation

7.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

7.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

7.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

8 Accuracy

8.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9 Storage limitation

9.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time.

9.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

9.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

9.5 You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10 Security integrity and confidentiality

10.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

10.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;
- Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and
- Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

10.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data].

11 How we define special categories of personal data

11.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

12 How we define processing

12.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

13 How will we process your personal data?

13.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

13.2 We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

14 Examples of when we might process your personal data

14.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

14.2 For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*; (* go to section 7.6)
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future; including social media and online postings (only of your images);
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time.

14.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose.

14.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

14.5 If we intend to process information about criminal convictions this will be explained at the appropriate time, along with the reasons for it in accordance.

14.6 We might process **special categories of your personal data** for the purposes in paragraph 7.2 above which have an asterisk (*****) beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

14.7 We do not take automated decisions about you using your personal data or use profiling in relation to you.

15 Retention of Personal Data

15.1 As explained in section 7 of this Policy, we have to process your data in certain circumstances, in order to do so the Company will have to retain your personal data.

15.2 Any personal data will be retained in accordance with the Company's security processes to minimise the risk of the data being used for unauthorised purposes.

15.3 To further reduce this risk the Company aims to irrevocably delete any data which it no longer needs. Where data was collected to achieve a specific objective, which has been met, shall be deleted.

15.4 The Company may often have need to retain data for longer periods of time to ensure that it is compliant with its legal and other obligations.

15.5 Any personal data shall not be kept for any period over and above 6 years from the date of termination of an employee's contract of employment (for services).

16 Sharing your personal data

16.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. Where we share your personal data with a third party we will keep a record of the data shared, the date that we shared it and the purpose for that data being shared.

16.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

16.3 The companies and agencies that may be informed of or provided with your personal data include: Ofsted, HMRC, our payroll providers, our employment law advisors, our computer service providers, our Accountants, Local Authorities, the Disclosing and Barring Service, Local Education Authorities, Training Agencies, Insurance Companies, the Police, the Border Agency, Recruitment Agencies, Banks, Regulation 44 Inspectors, vehicle rental companies, the Health and Safety Executive.

16.4 We do not knowingly send your personal data outside the UK. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained

17 Reporting a Personal Data Breach

17.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

17.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

17.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (your line manager). You should preserve all evidence relating to the potential Personal Data Breach.

18 Transfer limitation

18.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

18.2 You must comply with the Company's guidelines on cross-border data transfers.

18.3 You may only transfer Personal Data outside the UK if one of the following conditions applies:

- the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including:
    - the performance of a contract between us and the Data Subject;
    - reasons of public interest;
    - to establish, exercise or defend legal claims;
    - to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
    - in some limited cases, for our legitimate interest.

19 How should you process personal data for the Company?

19.1 Everyone who works for, or on behalf of, the Company has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies. Failure to follow any part of this policy could amount to misconduct or gross misconduct under our disciplinary procedure, which could result in your dismissal.

19.2 The Company's Managing Director acts as the Data Protection Officer and is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

19.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

19.4 You should not share personal data informally.

19.5 You should keep personal data secure and not share it with unauthorised people.

19.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

19.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

19.8 You should use strong passwords, keep passwords secure and not share passwords.

19.9 You should without exception lock your computer screens when not at your desk.

19.10 Personal data should be encrypted before being transferred electronically to authorised external contacts. If in doubt, speak to IT for more information on how to do this.

19.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

19.12 Do not save personal data to your own personal computers or other devices.

19.13 Personal data should never be transferred outside the UK except in compliance with the law and authorisation of the Data Protection Officer.

19.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

19.15 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

19.16 Personal data should be shredded and disposed of securely when you have finished with it.

19.17 You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

19.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

19.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

20 How to deal with data breaches

20.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

20.2 If you are aware of a data breach you must contact the Company's Data Protection Officer immediately and keep any evidence you have in relation to the breach.

21 Subject access requests

21.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer/ Manager who will coordinate a response.

21.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Company's Data Protection Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

21.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

22 Your data subject rights

22.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

22.2 You have the right to access your own personal data by way of a subject access request (see above).

22.3 You can correct any inaccuracies in your personal data. To do you should contact the Company's Data Protection Officer.

22.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Company's Data Protection Officer.

22.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Company's Data Protection Officer.

22.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

22.7 You have the right to object if we process your personal data for the purposes of direct marketing.

22.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

22.9 With some exceptions, you have the right not to be subjected to automated decision-making.

22.10 You have the right to be notified of a data security breach concerning your personal data.

22.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Company's Data Protection Officer.

22.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

23 Accountability

23.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

23.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;
- regularly training Company Personnel on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

24 Record Keeping

24.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

24.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record-keeping guidelines.

24.3 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

25 Training and audit

25.1 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

25.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Company's mandatory training guidelines.

25.3 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

26 Privacy by Design and Data Protection Impact Assessment (DPIA)

26.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

26.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

26.3 Controllers must also conduct DPIAs in respect to high-risk Processing.

26.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large-scale, systematic monitoring of a publicly accessible area.

26.5 A DPIA must include:

- a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

27 Automated Processing (including profiling) and Automated Decision-Making

27.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has Explicitly Consented;
- the Processing is authorised by law; or
- the Processing is necessary for the performance of or entering into a contract.

27.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

27.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

27.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

27.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

27.6 Where you intend to use any generative AI tool, you must also comply with the Company's Generative artificial intelligence in the workplace policy.

28 Direct marketing

28.1 We are subject to certain rules and privacy laws when marketing to our clients/service users.

28.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing service users known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

28.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

28.4 A Data Subject's objection to direct marketing must be promptly honoured. If a service user opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

29 Sharing Personal Data

29.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

29.2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

29.3 You may not share personal data with competitors, or personal acquaintances, or share it on social media in any format.

29.4 You may only share the Personal Data we hold with third parties, such as our service providers, if:

- they have a need to know the information for the purposes of providing the contracted services;

- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

30 Changes to this Data Protection Policy

30.1 We keep this Data Protection Policy under regular review.

30.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

----------END ----------

Physis Data Protection Policy & Data Consent

1. I have read and understood the contents of the enclosed Data Protection Policy and my personal responsibilities to uphold the requirements of Data Protection.

2. I hereby give consent for the company to collect, keep and process my personal data as given within the policy, especially as explained in clauses 2, 3, 13, 14, 15, and 16.

3. I will inform the company in a timely manner if there are any changes to my personal data.

4. I will abide by all the requirements of company's Data Protection Policy requirements but particularly with regards to clauses 1, 19, and 29.

5. I acknowledge that my failure to follow this Data Protection Policy could put the company at significant risk if it is found that the Data Protection Act 2018, or the UK General Data Protection Regulation (GDPR) is broken. Therefore, any misconduct in this area may be referred for investigation under the Disciplinary Policy.

Data Subject's name: **Role / relationship to Physis:**

Signed: **Date:**
