

This Data Sharing Agreement (“**DSA**”) sets out how “**we**” (also “**us**”; “**our**”; “**Medigold Health**”) and “**you**” (also the “**Customer**”; “**Client**”) will act with respect to the processing of Personal Data by each of us in connection with the Services provided under the Medigold Health [Standard Terms and Conditions of Supply](#) or such other terms and conditions of supply in force from time to time between you and us (also referred to as the “**Contract**” in this DSA).

This DSA is supplemental to the Contract but is maintained separately and may be updated by us from time to time. It has effect upon the creation of the Contract and the term of this DSA will mirror the term of the Contract. In case of any conflict or inconsistency between this DSA and the Contract (including any Order Form), this DSA will prevail unless otherwise expressly agreed between the parties.

1. Definitions

In this agreement:

“**Controller, Data Subject, Personal Data, Personal Data Breach, Processor, process/processing, Data Subject and Special Category Data**” each have the meaning given to them in UK GDPR (as defined below).

“**Controller Services**” means the Services to be provided by Medigold Health under the Contract in the capacity of Controller.

“**Controller Services Data**” means the Personal Data processed by the parties in the performance of the Controller Services.

“**Data Protection Laws**” means all applicable data protection and privacy legislation, regulations and guidance including:

- i. Regulation (EU) 2016/679) (as incorporated into UK legislation by way of the European Union (Withdrawal Agreement) Act 2020 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, together forming the “**UK GDPR**”) and the Privacy and Electronic Communications (EC Directive) Regulations 2003;
- ii. the Data Protection Act 2018; and
- iii. all applicable law about the processing of Personal Data and privacy;

and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

“**ICO**” means the UK Information Commissioner’s Office (including any successor or replacement body).

“**Order Form**” means any Order (as defined in the [Standard Terms and Conditions of Supply](#) (where applicable)).

“**Processor Services Data**” means the Personal Data processed by Medigold Health in the performance of the Processor Services.

“**Processor Services**” means the Services to be provided by Medigold Health in the capacity of a Processor where the Customer is the Controller.

“**Shared Controller Services Data**” means the Controller Services Data shared between the parties in the performance of the Controller Services, as further specified in clause 5 below.

Defined terms not otherwise defined in this DSA will have the meanings given in the Contract.

2. Controller Services

2.1 The parties expressly acknowledge and agree that both parties are independent Controllers in respect of their respective processing of Controller Services Data, on the basis that each party determines the purpose and means of processing that data.

2.2 When sharing Shared Controller Services Data, the parties will comply with the obligations set out in this DSA and the Data Protection Laws.

2.3 The parties agree that they will share Shared Controller Services Data pursuant to this DSA, to the extent necessary in connection with their respective purposes and functions, and as further set out in clause 5, Table B (Shared Controller Services Data).

2.4 The parties further agree that the Shared Controller Services Data will only be processed by them each respectively as far as is necessary according to their distinct purposes, in order to fulfil the obligations as set out in the Contract and otherwise only in compliance with the Data Protection Laws.

2.5 The parties will be individually and independently responsible for complying with all aspects of the Data Protection Laws when respectively processing Shared Controller Services Data. In particular, each party will be responsible for ensuring that it:

2.5.1 processes Shared Controller Services Data lawfully, fairly and transparently;

2.5.2 responds to requests from Data Subjects to exercise their Data Subject rights in respect of Shared Controller Services Data; and

2.5.3 retains Shared Controller Services Data for no longer than is necessary by reference to the purpose for which it is processed.

3. Processor Services

3.1 The parties expressly acknowledge and agree that the Customer acts as a Controller in respect of the Processor Services Data and Medigold Health as a Processor in respect of such data, on the basis that the Customer determines the purposes and means of processing the Processor Services Data and Medigold Health acts solely under the instructions of the Customer.

3.2 The parties acknowledge that for the purposes of the Data Protection Laws, Table A (Processor Services Data) at clause 5 sets out the scope, nature and purpose of processing by Medigold Health of the Processor Services Data including the duration of the processing and the types of Personal Data categories of Data Subject.

3.3 The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Processor Services Data to Medigold Health for the duration and purposes of this DSA.

3.4 Without prejudice to the generality of this clause 3, Medigold Health will, in relation to any Processor Services Data processed in connection with the performance by Medigold Health of its obligations relating to the Processor Services Data under this DSA:

3.4.1 process that Processor Services Data only to the extent and in such a manner as is necessary for the performance of the Contract in accordance with the written instructions of the Customer. Where Medigold Health believes the Customer's instructions do not comply with the Data Protection Laws, it will promptly notify the Customer;

3.4.2 maintain the confidentiality of the Processor Services Data and will not disclose the Processor Services Data to third parties unless it is necessary for the performance of the Services under the Contract or the Customer specifically authorises the disclosure, or as required by domestic law, court or regulator (including the ICO). If a domestic law, court or regulator (including the ICO) requires Medigold Health to process or disclose the Processor Services Data to a third party, Medigold Health must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless domestic law prohibits the giving of such notice;

3.4.3 ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of Processor Services Data and against accidental loss or destruction of, or damage to, Processor Services Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Processor Services Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Processor Services Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

3.4.4 ensure that all personnel who have access to and/or process Processor Services Data are obliged to keep the Processor Services Data confidential;

3.4.5 not transfer any Processor Services Data outside of the European Economic Area or the United Kingdom unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

- (a) the transfer is pursuant to an adequacy regulation or adequacy decision (as provided for under Article 45 UK GDPR or equivalent legislation) or the Customer or Medigold Health has provided appropriate safeguards in relation to the transfer;
- (b) the Data Subject has enforceable rights and effective legal remedies;
- (c) Medigold Health complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Processor Services Data that is transferred; and
- (d) Medigold Health complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Processor Services Data;

3.4.6 assist the Customer, at the Customer’s cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, Personal Data Breach notifications, impact assessments and consultations with supervisory authorities or regulators;

3.4.7 notify the Customer without undue delay on becoming aware of a Personal Data Breach affecting Processor Services Data that is likely to result in a risk to the rights and freedoms of natural persons;

3.4.8 at the written direction of the Customer, delete or return Processor Services Data and copies thereof to the Customer on termination of the Contract unless required by law to store the Processor Services Data; and

3.4.9 maintain complete and accurate records and information to demonstrate its compliance with this clause insofar as it relates to Processor Services Data and allow for audits by the Customer or the Customer’s designated auditor within mutually agreed timescales.

3.5 Upon written approval from the Customer, Medigold Health may appoint a third-party Processor subject to entering into a written agreement incorporating terms which are substantially similar to those set out in this clause. As between the Customer and Medigold Health, Medigold Health will remain fully liable for all acts or omissions of any third-party Processor appointed by it pursuant to this clause.

4. Miscellaneous

4.1 Both parties agree that they will at all times during the term of the Contract respect the medical confidentiality of the Customer’s personnel and comply with all relevant provisions of the Data Protection Laws and any statutory rules or instruments enacted or made pursuant to it.

4.2 Liability arising in connection with processing of Personal Data pursuant to this DSA, including in relation to loss or destruction of any of such Personal Data, will be in accordance with and subject to the limitation of liability provisions of the Contract (e.g. clause 12 of the [Standard Terms and Conditions of Supply](#)).

4.3 Notifications to Medigold Health in relation to this DSA should be sent to dpo@medigold-health.com. Notifications to the Customer will be sent to the contact specified on the Order Form or such other contact as notified in writing to Medigold Health by the Customer from time to time.

5. Data Processing Details

Table A – Processor Services Data

Categories of Data Subjects	Customer staff
-----------------------------	----------------

Types of Personal Data	• First and last name • Age • Sex • Employee number • Contact information (address, telephone number, and email address) • Role information / job specification • Employment history
Types of Special Category Data	Data concerning health such as background medical history, symptoms and ailments etc Racial or ethnic origin; Sex life or sexual orientation; and Trade Union membership (in each case only if relevant)
Nature and purposes of Processing	To provide the Processor Services
Duration of Processing	For the duration of the Contract insofar as it relates to Medigold Health's provision of Processor Services, save where Medigold Health is required to retain the Personal Data beyond the termination of the Contract where required by law and/or Medigold Health's retention policy.
Plan for return or destruction of Personal Data upon termination of the Contract	As set out in the DSA above.

Table A – Shared Controller Services Data

Description	Details
Categories of Data Subjects whose Personal Data it is necessary to share	Customer staff
Types of Personal Data it is necessary to share	• First and last name • Age • Sex • Employee number • Home address • Contact information (address, telephone number, and email address) • Role information / job specification • Employment history
Types of Special Category Data it is necessary to share	Data concerning health such as background medical history, symptoms and ailments etc. Racial or ethnic origin; Sex life or sexual orientation; and Trade Union membership (in each case only if relevant)
Necessity and purposes of data sharing	The Controller Services to be delivered under the Contract are intended to support the Customer in managing the health and wellbeing of individuals for whom it is responsible. It is therefore necessary for the Customer to share Shared Controller Services Data with Medigold Health (for example, through referral details), and for Medigold Health to collect and share Shared Controller Services Data with the Customer (for example, via reports or billing data) to fulfil each of their obligations.

Duration and retention of Shared Controller Services Data	As set out above, each party will be individually responsible for ensuring that Shared Controller Services Data is retained in accordance with Data Protection Laws.
--	--