

Data Processing Agreement

Data Processing Agreement where the customer is a business, company, institution, society or other undertaking. This agreement should be read alongside our Licence Agreement and does not apply to subscriptions purchased by individuals.

1. This agreement

- 1.1 **About us.** In this data processing agreement (DPA), references to **BMJ Group (us, we, or our)** are to **BMJ Publishing Group Limited** (company no. 3102371; registered office at BMA House, Tavistock Square, London WC1H 9JR; and VAT no. 674738491).
- 1.2 **Your contract with us.** This DPA is ancillary to our Licence Agreement and forms part of the legally binding agreement between us and **you** (the business, company, institution, society or other undertaking named in our Licence Agreement). This DPA sets out the additional terms, requirements and conditions upon which we will process the personal data we receive in connection with the BMJ Group products and services referred to in our Licence Agreement (together, the **Publications**) and should be read alongside our Licence Agreement.
- 1.3 **We may make changes to this DPA from time to time.** It is your responsibility to check this DPA periodically for any changes. Your continued use of the Publications means that you agree to any changes. This DPA was most recently updated on 1 October 2024.
- 1.4 **Translations.** Where this DPA has been translated into a language which is not English, this has been done for your convenience only to aid your interpretation. The English language version of this DPA shall prevail in the event of any conflict between the English language version and a version in any other language.

2. Definitions and interpretation

Expressions defined in our Licence Agreement and used in this DPA shall have the meaning set out in our Licence Agreement. In addition, the following defined terms are used in this DPA:

Data Protection Laws: means:

- **UK ONLY:** if your address (as specified in our Licence Agreement) is in the United Kingdom, the law of the United Kingdom which relates to the protection of personal data;
- **EEA ONLY:** if your address (as specified in our Licence Agreement) is inside the **European Economic Area**, the law of the United Kingdom which relates to the protection of personal data; and, where applicable, the law of the European Union or any member state of the European Economic area to which you are subject, which relates to the protection of personal data;
- **ROW ONLY:** if your address (as specified in our Licence Agreement) is outside the United Kingdom and **European Economic Area**, the law of the United Kingdom which relates to the protection of personal data; and, where applicable, the law of the jurisdiction in which you are based and to which you are subject, which relates to the protection of personal data.

Licence Agreement: means either: (a) where you have signed an agreement with us, those terms and conditions; or (b) your quotation from BMJ Group and the terms and conditions of our *Licence Agreement* (which is available on BMJ Group's website at <https://bmjgroup.com/legal-information/> and as updated from time to time).

Prohibited Purpose: any use or purpose that is unlawful, unfair, or which could unfairly override the interests or fundamental rights and freedoms of the data subjects involved.

Usage Data Purpose: the purpose(s) of: assessing usage of the Publications; recognising and managing continuing professional development; providing accreditation; providing learning support or learning management to Authorised Users; and/or providing other appropriate support, provided that the Usage Data Purpose excludes any Prohibited Purpose.

The terms **data controller**, **data processor**, **data subject** and **personal data** shall have the meanings as defined in the Data Protection Laws (and for the purposes of this DPA **personal data** shall comprise any the personal data set out in clause 3 below and any other personal data which we processes in connection with this DPA in BMJ Group's capacity as a data processor on behalf of you).

Any words following the terms including, such as, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms. Any obligation on a Party not to do something includes an obligation not to allow that thing to be done. Headings are used for convenience only and shall have no legal meaning or effect.

3. Personal data

The Parties have determined that, for the purposes of the Data Protection Laws:

We shall act as a data processor on your behalf in respect of the following personal data and processing activities:	
Types of personal data:	<p>Personal data shall include:</p> <ul style="list-style-type: none"> • Usage data • Any other data generated by Authorised Users' interactions with the Publications or any other BMJ Group products and services <p>In addition, where Authorised Users access the Publications in online format via access code registration, roaming access or mandatory personal account registration, personal data shall also include:</p> <ul style="list-style-type: none"> • Username (email address) • Password • Name • Country • Address (non-mandatory) • Phone number (non-mandatory) • Profession (mandatory for BMJ Learning) • Career grade (non-mandatory)
Categories of data subject:	Your Authorised Users and staff
Nature and scope of processing:	To fulfil our obligations to you as described in our Licence Agreement
Purpose of processing:	To fulfil our obligations to you as described in our Licence Agreement
Duration of processing:	For the duration of your Subscription Term

Should the above determination change, then each Party shall work together in good faith to make any necessary changes which are necessary to this clause.

4. Data protection compliance

Each Party shall comply with all applicable requirements of the Data Protection Laws. This clause is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Laws.

5. Your usage data

You may receive personal data pertaining to individual Authorised Users and their usage of the Publications. Where you receive any personal data from us, you undertake to use that personal data strictly for Usage Data Purposes only and not for any incompatible purpose or Prohibited Purpose.

6. Data processing obligations

6.1 You agree to (and shall take steps to ensure the lawful processing of personal data, including obtaining any required consents, from its personnel, representatives and agents, in respect of) all actions taken by us in connection with the processing of the personal data.

- 6.2 You will ensure that you take all necessary and appropriate steps (including obtaining any relevant consents and notices) to enable the lawful transfer of the personal data to us and lawful collection of the same by us for the duration and purposes of your licence.
- 6.3 In relation to the personal data, we shall:
 - 6.3.1 process that personal data only on your documented instructions, which shall be to process the personal data for the purpose(s) set out in clause 3 of this DPA, unless we are required by applicable laws to otherwise process that personal data;
 - 6.3.2 implement the technical and organisational measures set out in clause 7 below to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and otherwise to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, which you have reviewed and confirmed are 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;
 - 6.3.3 ensure that any personnel engaged and authorised by us to process personal data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;
 - 6.3.4 assist you insofar as this is reasonably possible (taking into account the nature of the processing and the information available to us), and at your cost and written request, in responding to any request from a data subject and in ensuring your compliance with your obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
 - 6.3.5 notify you without undue delay on becoming aware of a personal data breach involving the personal data;
 - 6.3.6 at your written direction, delete or return the personal data and copies thereof to you at the end of your Subscription Term unless we are required by applicable law to continue to process that personal data (and, for the purposes of this clause personal data shall be considered deleted where it is put beyond our further use); and
 - 6.3.7 maintain records to demonstrate our compliance with this clause 6.
- 6.4 You hereby provide your prior, general authorisation for us to:
 - 6.4.1 appoint data processors to process the personal data, provided that we shall: (a) ensure the terms on which we appoint such data processors comply with the Data Protection Laws, and are consistent with the obligations imposed on us in this clause 6; and (b) remain responsible for the acts and omission of any such data processor as if they were our acts and omissions.
 - 6.4.2 transfer the personal data outside of the United Kingdom as required for the purpose described in this clause 6, provided that we shall ensure that all such transfers are affected in accordance with the Data Protection Laws.

7. Security Requirements

The following technical and organisational measures shall apply:

Security of Transmission	We use Transport Layer Security, encryption at rest, encryption in transit. Our data protection and management policies cover how to transmit, and otherwise process personal data using our electronic systems.
Security of Storage	Our data protection and management policies cover how to store personal data using our electronic systems and standard retention periods.
Security of Processing	Our data protection and management policies cover how to process personal data using our electronic systems.
Organisational security measures	It is unusual for us to have hardcopies of personal data - usually only when printing information to review away from a computer. Our main office has managed entry and secure disposal facilities. Staff working from home can request paper shredders and secure home storage. Data management policies for both office-based and home-based workers are in place and updated yearly.

	Data protection and management policies also cover how to store, transmit, and otherwise process personal data using our electronic systems.
Technical security minimum requirements	We use Transport Layer Security, encryption at rest, encryption in transit. For the use of G-Suite products Google has provided a detailed list of what types of encryption applies to different types of processing and types of information. We use multi-factor authentication where it is available.
Updates to the Security Requirements	The Security Requirements will NOT update automatically if the information in our Licence Agreement is updated. The Parties must agree to any change(s) in writing.

8. International data transfers

This clause 8 shall not apply where you are established in any of the following territories: (i) the United Kingdom; (ii) a country within the [European Economic Area](#); or (iii) a country which the UK has determined offers an adequate level of data protection (a full list of which is available [here](#)).

8.1 The following additional defined terms are used in this clause 8:

International Data Transfer Addendum: the UK International Data Processing Addendum as issued by the UK Information Commissioner’s Office under section 119A(1) of the Data Protection Act 2018 (a copy of which is available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>).

Standard Contractual Clauses (processor to controller): the European Commission’s Standard Contractual Clauses for personal data transfers from an EU processor to controllers established in a third country (processor-to-controller transfers) as set out in the Annex to Commission Implementing Decision (EU) 2016/679 (a copy of which is currently available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914#d1e32-37-1).

8.2 This DPA incorporates the:

8.2.1 the [International Data Transfer Addendum](#) (including Part 2 *Mandatory Clauses*); and

8.2.2 the [Standard Contractual Clauses \(processor to controller\)](#).

8.3 The [International Data Transfer Addendum](#) and the [Standard Contractual Clauses \(processor to controller\)](#) shall be deemed to incorporate the information in the tables below. Where terms are used in this clause 8.3 which aren’t defined in this DPA or our Licence Agreement, those terms shall have the meaning given in the [International Data Transfer Addendum](#) or [Standard Contractual Clauses \(processor to controller\)](#) as relevant.

Part 1: Tables

Table 1: Parties

Start date	The Commencement Date specified in our Licence Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Key Contact	contractnotices@bmj.com	Your contact information as specified in our Licence Agreement

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:
-------------------------	---

Module 4 processor to controller	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Is personal data received from the Importer combined with personal data collected by the Exporter?
	x	x	x	x

Table 3: Appendix Information

<p>“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:</p>
<p>Annex 1A: List of Parties:</p> <ul style="list-style-type: none"> ● BMJ Publishing Group Limited ● You
<p>Annex 1B: Description of Transfer:</p> <p>Further to the information set out in clause 2 (<i>Usage Data Purpose</i>), and clause 3, institutional customers procure BMJ Group products and services for individuals. BMJ Group provides for those institutions to access user data. Where customer institutions wish to access user data they:</p> <ul style="list-style-type: none"> ● use the user data to support and monitor users, and to assess how users interact with BMJ Group products and services ● use the data solely for the purposes of education, to support users, and for research-to-publication measures; ● do not use the data in a way that is unfair or unlawful; ● inform users that the institution will be accessing the data, and explaining the reasons for doing so; ● explain to users any other organisations that the learner data will be disclosed to; and, ● comply with any national, regional, or other applicable laws when handling user data.
<p>Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Details as set out in Clause 7 of this DPA.</p>

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 19: Importer No Exporter Yes Neither Party No</p>
---	---

Part 2: Mandatory Clauses

The Parties agree that the “Alternative Part 2 Mandatory Clauses” of the [International Data Transfer Addendum](#) shall not apply.