Adept.

Data Processing Agreement

Last updated: 5th March 2026

This Data Processing Agreement ("**DPA**") forms part of, and is incorporated into, any agreement, proposal, statement of work, order, subscription, quotation, the Provider's standard Terms and Conditions, terms of business, or any other contract or arrangement governing the services (together, the "**Main Agreement**") between:

Adept Design (Norfolk) Limited ("**Provider**", "**Processor**", "**we**", "**us**", "**our**"); and
the client purchasing services from the Provider ("**Client**", "**Controller**", "**you**", "**your**").

This DPA applies where, and to the extent that, the Provider Processes Personal Data on behalf of the Client as a Processor in connection with the Services.

1. Definitions

In this DPA, unless the context requires otherwise:

Applicable Data Protection Law means all laws and regulations applicable to the Processing of Personal Data under the Main Agreement, including the UK GDPR, the Data Protection Act 2018, and, where applicable, the EU GDPR.

Client Personal Data means Personal Data Processed by the Provider on behalf of the Client in connection with the Services.

Data Subject, **Personal Data**, **Personal Data Breach**, **Process / Processing**, **Controller**, and **Processor** have the meanings given in Applicable Data Protection Law.

Services means the services provided by the Provider to the Client under the Main Agreement, including, where applicable, website development, hosting, support, maintenance, integrations, consultancy, software configuration, data migration, platform provision, and post-termination transition services.

Sub-processor means any third party appointed by the Provider to Process Client Personal Data on behalf of the Client in connection with the Services.

2. Scope and Role of the Parties

2.1 The parties acknowledge that the Client is the Controller and the Provider is the Processor in respect of Client Personal Data Processed by the Provider solely on the Client's behalf.

2.2 If, in relation to any specific activity, the Provider acts as an independent Controller (for example, for its own internal administration, billing, legal compliance, fraud prevention, security logging, or service improvement based on non-client-specific operational data), this DPA shall not apply to that Processing to the extent the Provider is not acting on the Client's behalf.

2.3 The subject matter, duration, nature and purpose of the Processing, and the types of Personal Data and categories of Data Subjects, are described in **Schedule 1**, as updated from time to time by the Main Agreement, applicable order, statement of work, or the Client's documented instructions.

2.4 The Client has the right to issue documented instructions, to receive breach notifications, to object to material Sub-processor changes, to request deletion or return at end of Services, and to audit in accordance with this DPA.

2.5 The Client is responsible for determining the purposes and means of Processing, ensuring a lawful basis and transparency obligations, and ensuring its instructions comply with Applicable Data Protection Law.

3. Client Instructions

3.1 The Provider shall Process Client Personal Data only on the documented instructions of the Client, including with regard to transfers of Client Personal Data to a third country or an international organisation, unless required to do so by applicable law.

3.2 The parties agree that the Main Agreement, statements of work, support requests submitted through agreed channels, system configuration choices made by the Client, and any written directions issued by authorised Client personnel constitute the Client's documented instructions.

3.3 If the Provider believes that an instruction infringes Applicable Data Protection Law, the Provider shall inform the Client without undue delay and may suspend implementation of that instruction pending clarification.

3.4 Where the Provider is required by applicable law to Process Client Personal Data otherwise than as instructed by the Client, the Provider shall (unless prohibited by law) inform the Client of that legal requirement before carrying out the Processing.

3.5 The Client is responsible for ensuring its instructions are lawful and that it has all necessary lawful bases, notices, and permissions to disclose Client Personal Data to the Provider and to permit the Provider to Process it in accordance with the Services.

4. Confidentiality

4.1 The Provider shall ensure that persons authorised to Process Client Personal Data are subject to appropriate obligations of confidentiality, whether contractual, statutory, or professional.

4.2 Access to Client Personal Data shall be limited to those personnel, contractors, and Sub-processors who require access for the performance of the Services.

5. Security

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risks to individuals, the Provider shall implement and maintain appropriate technical and organisational measures designed to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

5.2 Such measures may include, where appropriate:
(a) access controls and user authentication;
(b) least-privilege permissions;
(c) encryption in transit and/or at rest where reasonably appropriate;
(d) backup and recovery processes;
(e) system monitoring, logging, and security patching;
(f) staff confidentiality and security awareness measures; and
(g) appropriate supplier and hosting controls.

5.3 The Client acknowledges that no system can be guaranteed to be completely secure and that the Provider does not warrant uninterrupted or error-free operation.

6. Sub-processors

6.1 The Client grants the Provider general written authorisation to appoint Sub-processors in connection with the Services.

6.2 The Provider shall maintain an up-to-date list of Sub-processors (or categories of Sub-processors) used to deliver the Services, available on request or via the Provider's website.

6.3 The Provider shall give the Client reasonable prior notice of any intended material changes concerning the addition or replacement of Sub-processors (including by updating the list referenced in clause 6.2), thereby giving the Client the opportunity to object to such changes on reasonable and documented grounds relating to data protection.

6.4 If the Client objects in writing within 10 business days of being notified, the parties shall discuss the objection in good faith. Where the Provider cannot reasonably accommodate the Client's objection, the Client may terminate the affected Services by written notice, and the Provider shall provide end-of-service return/deletion in accordance with Section 12. No refund is due for fees properly incurred prior to termination.

6.5 The Provider shall ensure that any Sub-processor is bound by written terms requiring protection of Client Personal Data to a standard materially equivalent to this DPA, to the extent applicable to the services performed by that Sub-processor.

6.6 The Provider remains responsible for the performance of its Sub-processors to the extent required by Applicable Data Protection Law.

7. International Transfers

7.1 The Client authorises the Provider and its Sub-processors to Process Client Personal Data in the United Kingdom and, where necessary for the provision of the Services, in other countries.

7.2 Where the Provider transfers Client Personal Data to a country not recognised as providing an adequate level of protection under Applicable Data Protection Law, the Provider shall ensure that a lawful transfer mechanism is in place, such as appropriate contractual safeguards.

8. Assistance to the Client

8.1 Taking into account the nature of the Processing and the information available to the Provider, the Provider shall provide reasonable assistance to the Client to enable the Client to comply with its obligations under Applicable Data Protection Law, including in relation to:
(a) security of processing;
(b) Personal Data Breach notifications;
(c) data protection impact assessments;
(d) prior consultations with regulators where required; and
(e) responding to requests from Data Subjects.

8.2 Unless expressly included within the agreed scope of the Services, the Provider's assistance under this Section 8 (including meetings, advice, technical investigation, data extraction, compilation, reformatting, reporting, and project management) shall be chargeable at the Provider's then-current standard rates.

8.3 Clause 8.2 shall not apply to the extent that the assistance is required solely because of the Provider's proven breach of this DPA or Applicable Data Protection Law.

8.4 The Provider shall have no obligation to respond directly to any Data Subject unless required by applicable law or expressly agreed in writing.

8.5 Where the Client requires the Provider's assistance, the Client must provide full written particulars of the request. The Provider shall act within a reasonable timeframe, having regard to the nature, complexity, volume, and urgency of the request, the availability of relevant personnel, and the Provider's other operational commitments.

8A. Data Subject Rights

8A.1 Taking into account the nature of the Processing, the Provider shall provide reasonable assistance to enable the Client to respond to requests for exercising Data Subject rights under Applicable Data Protection Law (including access, rectification, erasure, restriction, portability, objection, and rights relating to automated decision-making).

8A.2 If the Provider receives a request directly from a Data Subject relating to Client Personal Data, the Provider shall (unless legally prohibited) promptly notify the Client and shall not respond directly except on the Client's documented instructions or as required by applicable law.

8A.3 Unless the Main Agreement expressly includes such assistance within scope, the Provider's assistance under this Section 8A (including locating, extracting, compiling, redacting, or exporting data) shall be chargeable at the Provider's then-current standard system administration rates, except to the extent the request arises solely due to the Provider's proven breach of this DPA or Applicable Data Protection Law.

9. Personal Data Breaches

9.1 The Provider shall notify the Client without undue delay after becoming aware of a Personal Data Breach affecting Client Personal Data and shall provide information reasonably available to it to assist the Client in meeting its legal obligations.

9.2 The Client acknowledges that detailed forensic investigation, remediation planning, audit support, regulator correspondence support, legal coordination, communications support, restoration work, and any enhanced reporting or consultancy are chargeable services unless the breach was caused solely by the Provider's proven breach of this DPA or Applicable Data Protection Law.

10. Audit and Information Rights

10.1 The Provider shall make available to the Client such information as is reasonably necessary to demonstrate compliance with this DPA.

10.2 The Client (or an independent auditor mandated by the Client) may audit the Provider's compliance with this DPA, subject to the following:
(a) at least 30 days' prior written notice, unless an audit is required by a competent supervisory authority or is reasonably necessary following a confirmed Personal Data Breach or credible security incident affecting Client Personal Data;
(b) audits shall be conducted during normal business hours and in a manner that minimises disruption and risk to the Provider's operations and other clients;
(c) audits shall be limited to the Processing of Client Personal Data and relevant controls;
(d) the auditor must be bound by confidentiality; and
(e) the Provider may require reasonable security and access measures.

10.3 The Provider may satisfy audit requests by providing relevant policies, summaries, and/or independent third-party reports or certifications where reasonable, and the parties shall agree in good faith a proportionate approach.

10.4 Unless the audit identifies a material breach of this DPA by the Provider, the Provider's reasonable time and costs incurred in supporting the audit (including staff time) shall be chargeable at the Provider's then-current standard system administration rates.

11. Change Requests, Non-Standard Work, and Response Times

11.1 The Client acknowledges that many data-related tasks are not automated self-service functions and may require technical analysis, manual intervention, bespoke scripting, data mapping, validation, testing, quality checks, export formatting, secure transfer preparation, or project management.

11.2 Accordingly, unless expressly included within the agreed scope of the Services, all such work is additional chargeable work at the Provider's then-current standard system administration rates.

11.3 The Provider does not guarantee to commence, complete, or deliver any data-related request within any particular period unless expressly agreed in writing.

11.4 The Provider shall perform requests under this DPA within a reasonable period, taking into account operational capacity, existing commitments, the complexity and scale of the work, security requirements, and any dependencies on third parties or legacy systems.

11.5 The Provider shall not be required to:
(a) prioritise the Client's request over other committed work without agreement;
(b) provide expedited, urgent, out-of-hours, or short-notice services unless agreed in writing; or
(c) incur material unplanned cost or resource allocation without the Client's agreement to applicable charges.

11.6 Where the Client requests accelerated delivery, urgent turnaround, or work outside normal business hours, the Provider may, at its discretion, agree to do so subject to an additional uplift or rush rate.

11.7 For the avoidance of doubt, references to "reasonable timeframe/period" in this DPA mean a timeframe that is reasonable in light of (a) the request scope, (b) data volumes, (c) technical feasibility, (d) security and verification requirements, (e) dependencies on third parties, and (f) the Provider's existing workload and resourcing. The Provider is not obliged to meet deadlines imposed unilaterally by the Client.

12. End of Services, Data Return, and Deletion

12.1 On termination or expiry of the Main Agreement, the Client may, by written notice, require the Provider to return or delete Client Personal Data in the Provider's possession or control, unless applicable law requires retention.

12.2 The Client must submit any request for return in writing and must specify, where applicable, the scope of data requested, preferred format (if any), delivery method, and verified recipient details. The Provider may require reasonable verification of authority and identity before releasing any data.

12.3 Unless otherwise agreed in writing, the Provider will return Client Personal Data in a reasonable and technically feasible format and via a secure method selected by the Provider. The Provider is not required to create new tools, bespoke exports, custom documentation, or complex migrations without an agreed paid scope.

12.4 The Client acknowledges and agrees that return, extraction, compilation, transformation, reformatting, validation, testing, packaging, transmission, migration assistance, and handover

support are chargeable at the Provider's then-current standard rates unless expressly included in the Main Agreement.

12.5 The Provider shall use reasonable endeavours to complete return or deletion within a reasonable period, taking into account volume, complexity, feasibility, security requirements, third-party dependencies, and the Provider's operational capacity. The Provider does not guarantee fixed turnaround times unless expressly agreed in writing.

12.6 The Provider is not required to commence return work until (a) the Client's request is sufficiently clear, (b) any applicable fees, estimate, deposit, or charging basis has been agreed, and (c) necessary security and access requirements are satisfied.

12.7 If the Client does not request return of Client Personal Data within 30 days of termination/expiry (or such other period stated in the Main Agreement), the Provider may securely delete Client Personal Data in accordance with its retention and deletion practices, subject to applicable law.

12.8 The Provider may retain (a) data required by law, (b) data required to establish, exercise, or defend legal claims, and (c) billing, contractual, and audit records. Client Personal Data remaining in backups and archives will be protected and put beyond use and will be deleted or overwritten in accordance with the Provider's ordinary backup lifecycle, and will not be restored or actively processed except as necessary for disaster recovery testing, security, integrity, or legal compliance.

13. Client Warranties and Responsibility

13.1 The Client warrants that it has all necessary rights, lawful bases, and authority to instruct the Provider to Process Client Personal Data under the Main Agreement and this DPA.

13.2 The Client shall indemnify and keep indemnified the Provider against any losses, costs, claims, liabilities, and expenses arising out of or in connection with:
(a) unlawful or unauthorised Client instructions;
(b) the Client's failure to obtain required notices, consents, permissions, or lawful bases;
(c) inaccurate, excessive, or unlawfully collected Client Personal Data; or
(d) the Client's breach of Applicable Data Protection Law,

except to the extent caused by the Provider's breach of this DPA.

14. Liability

14.1 This DPA is subject to the liability and exclusion provisions of the Main Agreement.

14.2 If the Main Agreement does not contain liability provisions, the Provider's aggregate liability arising under or in connection with this DPA shall be limited to the total fees paid or payable by the Client under the Main Agreement in the 12 months preceding the event giving rise to the claim.

14.3 Nothing in this DPA excludes or limits liability which cannot lawfully be excluded or limited.

15. Order of Precedence

15.1 If there is any conflict between this DPA and the Main Agreement in relation to the Processing of Personal Data by the Provider as Processor, this DPA shall prevail to the extent of that conflict.

15.2 For commercial matters including fees, rates, payment terms, service scope, and response times, the Main Agreement shall prevail unless this DPA expressly states otherwise.

16. General

16.1 This DPA shall commence on the date the Provider first Processes Client Personal Data on behalf of the Client and shall continue until such Processing has ceased.

16.2 The Provider may update this DPA from time to time by publishing an updated version on its website or otherwise notifying the Client, provided that any updated version shall not materially reduce the level of protection for Client Personal Data where the Provider is acting as Processor, except where required to reflect changes in law, regulation, guidance, technology, Sub-processors, or service delivery models.

16.3 If any provision of this DPA is held invalid or unenforceable, the remainder shall continue in full force and effect.

16.4 This DPA shall be governed by the law governing the Main Agreement, or if none is specified, the laws of England and Wales.

Schedule 1: Description of Processing

A. Subject Matter of the Processing

The provision of digital, technical, creative, hosting, support, maintenance, platform, consultancy, migration, and related services by the Provider to the Client.

B. Duration of the Processing

For the duration of the Main Agreement and any additional period during which the Provider retains Client Personal Data in accordance with the Main Agreement, this DPA, or applicable law.

C. Nature and Purpose of the Processing

The Provider may Process Client Personal Data for the following purposes, to the extent relevant to the Services:

- website hosting and operation;
- website and software development;
- content management and publishing;
- user account management;
- customer relationship and communication functions;
- form handling and enquiry processing;
- email delivery and notification services;
- analytics, diagnostics, and performance monitoring;
- support, maintenance, and troubleshooting;
- backups, disaster recovery, and business continuity;
- security monitoring and access control;
- integrations with third-party systems;

- data migration, import, export, extraction, and transfer;
- software platform administration and configuration;
- reporting and database management;
- post-termination handover, deletion, or return activities requested by the Client.

D. Types of Personal Data

As determined by the Client and the Client's use of the Services, which may include:

- names;
- contact details;
- email addresses;
- telephone numbers;
- postal addresses;
- IP addresses and device/browser identifiers;
- account credentials or authentication-related data;
- transaction or interaction records;
- form submissions and correspondence;
- profile information;
- marketing preferences;
- technical logs;
- any other Personal Data submitted, stored, transmitted, or otherwise made available by the Client through the Services.

E. Categories of Data Subjects

As determined by the Client and the Client's use of the Services, which may include:

- the Client's customers and prospective customers;
- website users and visitors;
- employees, contractors, and representatives;
- members, donors, supporters, or subscribers;
- event attendees;
- suppliers and business contacts;
- any other individuals whose Personal Data the Client chooses to Process through the Services.

F. Special Category Data

The Client shall not provide Special Category Data to the Provider unless expressly agreed in writing and only where appropriate safeguards and instructions are in place.