



Processing addendum

Client Personal Data

Version 3.0 | Effective date 01/08/2026 | Disruption Works Ltd

Instructions and safeguards

This edition is effective from 01/08/2026 and forms part of the service agreement when expressly agreed. It applies where Disruption Works Ltd processes personal data on the client's behalf, including authorised development, deployment or support access in the client's cloud. It continues until that processing and the agreed return or deletion are complete.

1 Scope and roles. The completed processing schedule in the order describes the subject, duration, nature and purpose of processing, data types, categories of individuals, locations, approved suppliers and security controls. The client is controller, or a processor authorised by its controller to appoint DW as subprocessor. DW acts as processor or subprocessor accordingly. Independent business-contact processing is outside this addendum and is governed by each party's own obligations.

Applicable data-protection law means the UK GDPR, Data Protection Act 2018 and other privacy laws applicable to the processing, as amended from time to time. Terms such as controller, processor, personal data and personal data breach have their statutory meanings. The client's rights include giving lawful instructions, receiving assistance, auditing and directing return or deletion as set out here; it is responsible for the lawful basis, required notices and authority for its instructions.

2 Documented instructions. DW will process data only on the client's documented instructions, including instructions about transfers, unless applicable law requires otherwise. DW will notify the client before legally required processing unless prohibited by law. DW will promptly flag instructions it considers unlawful and may pause the affected processing while the parties resolve them. The agreement does not authorise unrelated analytics, advertising, sale of data or general model training.

3 People and security. DW will restrict access to authorised people who need it for the agreed work and are bound by confidentiality. DW will implement appropriate technical and organisational measures meeting applicable law and the completed security schedule, taking account of the risks, nature of processing and available technology. Measures apply to DW's activities even where the data is hosted by the client.

The schedule must identify access controls, encryption, secrets management, separation, logging, secure development, vulnerability handling, backup and recovery responsibilities. DW will maintain and review the measures within its scope and will not materially reduce agreed protection. Client control of a tenant does not remove DW's responsibility for its own credentials, access or actions.

4 Assistance and incidents. Taking account of the processing and information available, DW will provide appropriate assistance with individual rights, security, breach assessment and notification, impact assessments and prior consultation with regulators. DW will promptly forward requests concerning client data and not respond substantively without instruction unless law requires it.

DW will notify the client's incident contact without undue delay after becoming aware of a personal data breach affecting the processing. It will provide available details of the event, affected data and individuals, likely consequences, contact point and mitigation, with updates as facts develop. DW will preserve relevant evidence and cooperate in containment and recovery. The client makes notifications for which it is legally responsible; this does not remove DW's own legal duties. An arbitrary waiting period or lack of a completed investigation does not delay initial notification.

Suppliers and AI processing

5 Subprocessors. The client authorises only the DW subprocessors identified in the completed schedule at agreement. DW will give at least 30 days' prior written notice of additions or replacements, describing the entity, service, data and location. The client may object within 10 business days on reasonable data-protection grounds. The parties will seek a suitable solution; the new provider must not process the affected data while a timely objection remains unresolved. If no solution is agreed, either party may end the affected service and charges are settled under the service terms.

DW will impose written obligations providing the protection required by applicable processor law on its subprocessors and remains responsible to the client for their performance of those obligations. General exclusions for external-provider failures do not remove this responsibility. Suppliers contracted directly by the client are classified according to their actual role and instructions; they are not automatically DW subprocessors.

6 Commercial AI restrictions. OpenAI, Anthropic, Google Gemini and Microsoft Azure OpenAI are principal provider options, not automatic approvals. Each selected service and contractual route must be identified in the schedule. DW will use only approved commercial arrangements that prohibit training or improvement of general-purpose or shared models using client inputs, outputs, files and other content, and prohibit sale or disclosure beyond the authorised delivery chain.

DW will not opt into voluntary training, feedback or data-sharing programmes. Client-specific fine-tuning requires separate documented instructions and controls; it is not included in general approval to use AI. Consumer tools and unapproved free services must not receive client personal data.

Permitted service delivery, security and support processing, including authorised subprocessors, must be recorded. The schedule must separately disclose retention, abuse monitoring and human review, feature storage, processing locations and any legal retention. No-training does not mean zero retention. Where a selected route cannot meet the required restrictions, DW will not use it for the affected data. If a material contractual or technical change undermines those restrictions, DW will notify the client and suspend affected processing until an approved compliant arrangement is in place.

7 International transfers. DW will not make a restricted international transfer without the client's documented authorisation and a valid legal mechanism, together with required assessment and safeguards. The schedule records the actual processing chain and relevant storage, inference and remote-support locations. As applicable, the parties will use adequacy provisions or the relevant official UK IDTA, UK Addendum to EU standard contractual clauses, or other lawful mechanism, completed for the actual transfer. EU requirements are addressed separately where applicable.

This addendum is not itself an international transfer instrument. Any required official instrument must be completed and executed before the transfer. Its mandatory provisions take priority. A vendor name, UK billing account or selected storage region is not evidence that all processing stays in that region.

Evidence and exit

8 Records and audit. DW will maintain the records required by law and provide information reasonably needed to demonstrate compliance with this addendum. It will allow and contribute to audits and inspections by the client or its independent auditor. Routine audits should use existing relevant evidence where sufficient and give reasonable notice, normally 10 business days. Urgent incident, suspected material non-compliance and regulatory audits are not constrained by that notice or a fixed annual limit.

Audits must protect other clients' data and confidentiality and avoid unnecessary disruption, without preventing effective verification. DW will promptly address identified non-compliance within its responsibility. Ordinary compliance information is included in the service. Additional assistance may be charged at agreed reasonable rates where not caused by DW's breach; charges must not obstruct statutory rights or required urgent assistance. DW bears the cost of correcting its own breach.

9 Return and deletion. At the client's choice, DW will return or securely delete the personal data and existing copies when the services end, unless applicable law requires retention. The schedule states the return format, timetable and backup deletion cycle. Unless a different timetable is agreed, DW will complete active-system return or deletion within 30 days of instruction. A client's statutory or urgent lawful requirements take priority where they require faster action.

Backups that cannot reasonably be selectively erased must be isolated from ordinary use, remain protected and expire under the documented cycle. If restored, the deletion instruction must be reapplied. Any legally retained data must be limited to what is required, protected and not used for another purpose. DW will confirm completion on request. This does not authorise DW to delete systems or data in the client's tenancy without the client's instructions.

10 Liability and priority. The service terms govern contractual liability between the parties only to the extent lawful. They do not reduce obligations under mandatory transfer terms or rights of data subjects and regulators. This addendum prevails over inconsistent service terms for personal-data matters. It can be changed only by written agreement, subject to mandatory law.

Processing schedule completion

The Service order contains the schedule to complete and incorporate. Before processing starts, both parties must confirm the purposes and duration; data and individuals; roles; authorised instructions; actual security measures and responsibility split; AI provider contracts and settings; other subprocessors; locations and transfer arrangements; retention and backup cycles; return or deletion; and incident contacts.

No production personal data is authorised for a provider or feature whose required safeguards or processing details remain unapproved. Testing should use synthetic or appropriately anonymised data until those conditions are met.