PIMS Workspace Terms and Conditions

These publication terms contain the SaaS clauses and service and data-processing schedules. Customer-specific commercial particulars and acceptance are recorded separately in the agreed Order Form.

Supplier: Data Privacy and Data Security Services Limited (Trading as Data Privacy Services). Registered company number HE 432380. Registered address: Griva Digeni, 51 Athineon Court, Office 202, 8047, Paphos, Cyprus. Contact: info@dataprivacyservices.co.uk. The Supplier is referred to as DPS in this agreement.

SaaS licence and subscription

1 Agreement and definitions

1.1 The agreement comprises the accepted Order Form, these terms and schedules. It is for organisations acquiring services for business or professional purposes. A person accepting for the Customer must have authority to bind it. It takes effect on signature or another recorded acceptance expressly identifying this version; mere browsing does not constitute acceptance.

1.2 Customer Data means data, documents and other content submitted by or for the Customer, including personal data. Authorised Users are people the Customer authorises for its own workspace, including employees, contractors and auditors. The Service is the hosted PIMS Workspace identified in the Order Form. Applicable Data Protection Law means EU GDPR, UK GDPR, the UK Data Protection Act 2018 and relevant Cyprus or other applicable data protection legislation, as amended.

1.3 Mandatory law and any applicable international transfer clauses prevail. Schedule 2 prevails on personal data protection matters, Schedule 1 on service levels, and the Order Form on expressly agreed commercial particulars. A signed variation prevails only to the extent it identifies the provision being varied. Website marketing or later online changes do not unilaterally vary a signed agreement.

2 Organisation licence and service scope

2.1 DPS grants the Customer a non-exclusive, non-transferable right for the subscription term to access and use the Service for the licensed organisation’s internal purposes. The fee buys organisational access to the software, not individual user licences. DPS will not charge by user count under the basic licence. Separate legal entities or group companies require express inclusion in the Order Form.

2.2 Software to support ISO 27701:2025 implementation and ongoing privacy information management through the processes, documentation, registers, governance and tasks listed in the agreed feature specification. Access begins only when DPS makes the contracted service available; a demonstration or development preview does not start a paid subscription.

2.3 The basic licence includes UK hosting, routine software maintenance and updates, and technical support under Schedule 1. It excludes implementation consultancy, managed compliance, ongoing management support, outsourced DPO services, bespoke development, migration services and certification or external audit fees. These may be purchased under a separate written statement of work. Statutory processor assistance in Schedule 2 remains applicable.

3 Term and renewal

3.1 The initial subscription lasts at least 12 months from the service commencement date in the Order Form. A 12-month period ends on the day before its anniversary. A longer initial period applies only if expressly agreed. Monthly billing is an instalment arrangement for the whole committed term and does not create a monthly cancellable subscription.

3.2 Each subscription automatically renews for successive 12-month terms unless the Customer gives written non-renewal notice at least two calendar months before the current term end date, or the agreement ends under

section 8. DPS may elect not to renew by giving at least the same notice. The Order Form must state the actual term end and notice deadline. A notice received on the deadline is timely.

3.3 Give notices to the addresses in section 11. DPS will send a renewal reminder at least three calendar months before term end. The reminder does not replace the Customer's obligation to give notice. Non-renewal stops the next term; it does not cancel charges for the current term.

3.4 No voluntary cooling-off period is offered for a business subscription. Any statutory cancellation, withdrawal or cooling-off right that applies is preserved, including its required notice, refund and service commencement rules. Such a right takes priority over the minimum term and renewal provisions to the extent required by law.

4 Fees and payment

4.1 Fees, currency, billing frequency, payment dates and taxes are specified in the Order Form. Annual fees may be billed upfront or in agreed monthly instalments. Fees remain due for the committed term, subject to statutory rights and the express termination and refund provisions below. DPS must notify any renewal price change at least three calendar months before term end; otherwise existing prices continue for that renewal unless both parties agree otherwise.

4.2 The Customer must promptly identify any disputed invoice and pay undisputed amounts when due. The parties will investigate genuine disputes. DPS will not suspend solely for an amount reasonably disputed in good faith while the Customer cooperates with that investigation.

4.3 A one-time customer setup fee is payable in addition to the licence fee, with its amount, currency, scope and payment due date specified in the Order Form. It is not charged again on an ordinary annual renewal. Implementation consultancy and ongoing management support remain separate services.

Using the workspace

5 Customer responsibilities

5.1 The Customer chooses its administrators and Authorised Users and remains responsible for their use, permissions, lawful content and instructions. Administrators must use appropriate roles, remove access promptly when no longer needed and review guest and auditor expiry dates. The organisation licence does not permit public resale, service bureau use, sublicensing or access for an unlicensed organisation.

5.2 Users must have individual accounts, complete two-factor authentication and keep their credentials secure. Shared logins and attempts to access another client's workspace are prohibited. The Customer must promptly report suspected compromise and keep its contact details, endpoints and internet connectivity suitable for secure access.

5.3 The Customer must not upload unlawful content, malicious code or material it has no right to use, bypass security, disrupt the Service, conduct unapproved penetration testing or copy or reverse engineer the software except where a non-excludable legal right permits this. Any reasonable storage or usage limits must be stated in the Order Form; DPS may not introduce per-user fees through a fair-use provision.

5.4 The Customer determines its compliance decisions, risk acceptance, approvals, retention periods and evidence accuracy. Templates and guidance need organisational review and adaptation. The Service assists implementation and management; it does not itself confer certification, accreditation or a guarantee of legal compliance. Auditing and certification remain the responsibility of the relevant independent bodies.

5.5 AI functions, where contracted and enabled, provide assistance and require appropriate human review. The Customer must avoid submitting unnecessary personal data and verify outputs before relying on them. DPS may process Customer Data through an AI provider only in accordance with the documented instructions, approved subprocessors and transfer arrangements in Schedule 2. DPS will not use Customer personal data to train general-purpose AI models without a separate lawful, explicit written instruction and the required safeguards.

6 Ownership and permitted use

6.1 The Customer retains ownership of Customer Data. DPS receives only the rights needed to host, secure, support and provide the Service and perform this agreement. No data sharing provision transfers ownership or permits DPS to sell Customer Data or use it for advertising.

6.2 DPS and its licensors retain rights in the software, branding and supplied template materials. The Customer may adapt the supplied templates for its own business and retain its completed policies, records and exported Customer Data after termination. It may not redistribute DPS's unmodified template library commercially. Rights in third-party standards and licensed materials remain with their owners.

7 Confidentiality and service changes

7.1 Each party must protect the other's confidential information using reasonable care, use it only for this agreement and disclose it only to people with a legitimate need who owe confidentiality duties. The duties do not cover information lawfully public, already lawfully known, independently developed or lawfully received without restriction. Required legal disclosure is permitted, with prior notice where lawful and minimum necessary disclosure.

7.2 DPS may improve the software and apply security patches but must not materially reduce contracted core functionality, security or data export capability during a paid term. Material adverse changes require advance notice and agreement or an appropriate remedy. Emergency security changes may take effect immediately, with notice as soon as practical.

7.3 DPS will perform the Service with reasonable skill and care and in accordance with the SLA and data protection obligations. The Customer must report defects with enough information for investigation. DPS will correct reproducible defects affecting contracted functionality within a reasonable period, prioritising their severity. No promise is made that every minor defect will be resolved in 24 hours.

Ending the contract and legal terms

8 Suspension and termination

8.1 DPS may suspend affected access where reasonably necessary to contain a security threat, unlawful use or material risk to other clients. Suspension must be proportionate and limited to affected functions or users where practical. DPS will notify the Customer promptly, explain the reason where lawful and restore access when the cause is resolved. It remains responsible for protecting retained Customer Data.

8.2 For overdue undisputed fees DPS must give at least 14 days' written notice and an opportunity to pay before suspension. Either party may terminate for a material breach not remedied within 30 days after written notice identifying it. Either may terminate immediately for a breach incapable of remedy or insolvency, subject to applicable insolvency law.

8.3 The Customer may terminate the affected subscription for repeated SLA failure under Schedule 1. Where termination results from DPS's unremedied material breach or an SLA termination right, DPS will refund prepaid fees for the unused period from termination and cancel future instalments for that period. Otherwise fees for the committed term remain payable, subject to mandatory law. Termination does not extinguish accrued rights.

8.4 On expiry or termination, ordinary user access ends and the Customer must stop using the software. DPS will provide the export and deletion process in Schedule 2. It will not withhold Customer personal data solely because fees are disputed. Transition work beyond the standard export is chargeable only under a separately agreed quotation. Data protection, confidentiality, accrued payment obligations and provisions intended to survive continue as necessary.

9 Liability

9.1 Neither party limits liability for fraud, fraudulent misrepresentation, deliberate misconduct, gross negligence, death or personal injury caused by negligence, or any liability that applicable law prohibits it from limiting. Nothing limits a data subject's rights, regulatory powers or a party's direct statutory responsibilities under data protection law.

9.2 Subject to section 9.1, each party's total contractual and non-contractual liability arising from this agreement in any subscription year is limited to the total fees paid or payable for the affected workspace for that 12-month subscription year. For breach of confidentiality or Schedule 2, a separate cap of twice those fees applies instead. Related events are treated as one event in the year in which the first occurs. Customer obligations to pay agreed fees are not reduced by these caps.

9.3 Subject to section 9.1, neither party is liable for indirect or consequential loss or loss of anticipated profit. Reasonable, necessary direct costs of restoring Customer Data following DPS's breach and responding to a personal data breach are not excluded merely because they relate to data. A statutory contribution claim between controller and

processor remains available to the extent applicable law requires.

10 Events outside control and disputes

10.1 A party is excused only to the extent an event genuinely beyond its reasonable control prevents performance despite reasonable safeguards and mitigation. Ordinary supplier failure, inadequate capacity or lack of funds is not automatically such an event. The affected party must notify the other, mitigate and resume promptly. If material inability to provide the Service continues for 30 days, either party may terminate the affected service and DPS will refund unused prepaid fees. Data protection duties continue to the extent legally required.

10.2 The parties will first refer disputes to authorised managers and attempt resolution for 30 days, without preventing urgent relief or regulatory complaints. This agreement is governed by Cyprus law and subject to the exclusive jurisdiction of the courts of Cyprus, except for mandatory jurisdiction, statutory rights and applicable transfer-clause requirements that cannot be displaced.

11 Notices and general provisions

11.1 Send contractual notices, including non-renewal, to info@dataprivacyservices.co.uk for DPS and to the notice email in the Order Form for the Customer. Email notice is effective on receipt, evidenced by acknowledgement or successful delivery without a failure notification. Retain delivery evidence; if delivery is uncertain, use tracked post to the registered address. DPS must acknowledge non-renewal promptly. Technical tickets alone are not contractual notices.

11.2 Changes require written agreement except changes expressly allowed here. Neither party may assign the agreement without the other's written consent, not unreasonably withheld. Invalid provisions are severed only as necessary. Failure to exercise a right is not a waiver. The agreement contains the whole agreement on this service, without excluding fraud. Electronic acceptance and counterparts are valid to the extent permitted by law.

Schedule 1 Service level agreement

This SLA covers the paid production Service from commencement. Demonstrations and development previews are excluded.

Measure	Commitment
Technical support response	Initial human response within 24 elapsed hours of ticket receipt
Monthly availability	Minimum 95 percent uptime
Availability objective	99.9 percent uptime — objective rather than guaranteed minimum
Routine maintenance and updates	At weekends, using UK local time
Recovery point objective	RPO of 24 hours
Recovery time objective	RTO of 8 hours

S1 Support and escalation

Submit tickets through workspace Support, or email info@dataprivacyservices.co.uk if unavailable. Include organisation, issue, impact and contact details; omit passwords and unnecessary sensitive data. The 24-hour clock includes weekends and holidays. A human must acknowledge, assess and give the next action; an automated receipt is insufficient. This is a response commitment, not a resolution deadline.

DPS prioritises outages, compromise and data loss, provides proportionate updates and escalates serious incidents to its service manager. After 24 hours without response, escalate to the same email with the ticket reference. Support covers software faults, access and service incidents; compliance consultancy and management are separate services.

S2 Availability and maintenance

Measure availability per workspace each calendar month: uptime percent = 100 × (total monthly minutes − unavailable minutes) ÷ total monthly minutes. Unavailability means inability to sign in or use a contracted core function due to DPS's service or hosting. DPS uses monitoring and substantiated Customer reports and provides the calculation on request.

Scheduled maintenance downtime counts as unavailable minutes in the 95 percent calculation. Routine maintenance and updates occur on Saturdays or Sundays in UK local time, with at least 48 hours' notice where interruption is expected. Critical security fixes may occur outside that window; DPS gives notice as soon as practical and counts resulting interruption. Customer-only connectivity or device failures, Customer-caused access restrictions and a valid suspension for Customer breach are excluded only to the extent they cause the interruption; DPS records the reason and duration. Infrastructure provider SLAs do not replace this SLA.

S3 Recovery and service failure

DPS will maintain backups and recovery procedures to meet an RPO of 24 hours and RTO of 8 hours. RPO is the maximum period of Customer Data changes that may be lost, measured backwards from the disruption. RTO is the maximum elapsed time to restore core access and recover Customer Data following a recoverable disruption, measured from the beginning of the outage as established by monitoring or substantiated reports. DPS will restore from a safe recovery point, validate access and data integrity, and report any data loss and recovery time.

DPS will test recovery arrangements periodically and disclose material limitations before contracting. The commitment does not represent an assurance of automatic regional failover. If wider infrastructure disruption prevents recovery within eight hours, DPS must escalate, keep the Customer informed and record the SLA breach; that disruption is not automatically excluded merely because a hosting supplier is involved. Section 10.1 applies only where its conditions are satisfied.

After a missed SLA DPS will investigate, provide a corrective action summary and take reasonable steps to prevent recurrence. The Customer may terminate the affected subscription if uptime is below 95 percent in two consecutive months or three months in a rolling six-month period, by notice within 30 days of the relevant report. Section 8.3 applies. No automatic service credit is specified unless agreed in the Order Form; this does not remove other contractual or statutory remedies.

Schedule 2 Data Processing and Data Sharing Agreement

D1 Roles and scope

For Customer personal data processed through the Service, the Customer is the Data Controller and DPS is the Data Processor. This schedule is the parties' controller–processor agreement under Article 28 of EU GDPR and UK GDPR where applicable. Data sharing under it is limited to processing on the Customer's behalf and authorised disclosure; it does not create joint controllership or give DPS an independent purpose for using workspace content.

Where the Customer acts for another controller, it must have authority to appoint DPS as a subprocessor and issue instructions. DPS then performs the same processor duties in this schedule and the Customer passes on the relevant controller instructions. Each party remains responsible for its own statutory obligations. Processing details and security measures are in Schedule 3; authorised subprocessors and locations are in Schedule 4.

DPS acts as an independent controller only for information it needs for its own billing, business contact administration and compliance with its legal obligations. It must identify that processing in its privacy notice and establish a lawful basis. This limited role does not authorise reuse of Customer workspace content for DPS's own purposes. Service operational records processed to provide and secure the Customer's workspace fall within the processor scope unless a distinct lawful controller purpose is documented.

D2 Documented instructions and confidentiality

The agreement, completed schedules, Customer configuration choices and written requests from authorised Customer contacts are the documented instructions. DPS must process personal data only on those instructions, including instructions on disclosures and international transfers. If EU or Member State law requires other processing, DPS will notify the Customer of that requirement before processing unless the law prohibits notification for important public interest reasons.

DPS must immediately inform the Customer if it considers an instruction infringes Applicable Data Protection Law and may pause the affected processing while the parties resolve it. It must not silently substitute its own purpose. Additional instructions that materially change scope or cost require an agreed variation, without delaying urgent legally required assistance.

DPS must restrict access to authorised personnel who need it for their duties, ensure they are bound by contractual or statutory confidentiality, give appropriate data protection and security training, and remove access when no longer required. Those obligations continue after personnel leave or the contract ends.

D3 Subprocessors and recipients

The Customer gives general written authorisation only for subprocessors identified in the completed Schedule 4 and additions or replacements made through this procedure. DPS must give at least 30 days' advance written notice of a proposed change, identifying the legal entity, function, processing location, security arrangements and transfer mechanism. The Customer may object on reasonable data protection grounds during that period.

DPS must address a reasonable objection before the new subprocessor receives the affected data, for example by using an alternative or disabling the affected optional feature. If no compliant solution is available, the Customer may terminate the affected service before the change takes effect and receive unused prepaid fees back. Silence after proper notice may constitute no objection under this general authorisation; it does not authorise undisclosed processing.

DPS must impose equivalent data protection obligations on subprocessors through a binding written contract, verify sufficient safeguards and remain fully liable to the Customer for their performance of those obligations. It must maintain an accurate list, including relevant further subprocessors, and provide it on request. DPS will not disclose content to another client or outside recipient unless instructed or legally required. Customer-authorised auditors and integrations receive only the access and data the Customer approves.

Processor assistance and accountability

D4 Security and incidents

DPS must implement and maintain appropriate technical and organisational measures under Article 32, taking account of processing risks, and at least the measures in Schedule 3. It must not materially reduce protection during the term. DPS will assess and test safeguards, maintain processing records where required, cooperate with supervisory authorities and make relevant compliance evidence available to the Customer.

DPS must notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer personal data, and in any event provide an initial notification within 24 elapsed hours of awareness. This contractual notification period does not permit avoidable delay. DPS need not wait for a complete investigation. The notification goes to the Customer privacy and emergency contacts in the Order Form and must use a suitable secure channel.

DPS will provide, as known, the nature of the breach, affected data and data subject categories and approximate numbers, likely consequences, mitigation and containment measures, and a contact for follow-up. It will provide missing information in stages without undue delay, preserve relevant evidence, cooperate in investigation and keep the Customer informed. The Customer decides and makes controller notifications to regulators and individuals unless law requires DPS to notify directly. DPS's processor notice must not be confused with the controller's applicable regulatory deadline.

D5 Rights requests and compliance assistance

Taking account of the nature of processing, DPS must assist the Customer through appropriate technical and organisational measures with requests to exercise data subject rights, including access, correction, erasure, restriction, objection and portability where applicable. DPS must promptly forward requests it receives concerning Customer Data and must not respond substantively without instruction unless legally required.

Taking account of the processing and information available to it, DPS must assist the Customer with security, breach notification, data protection impact assessments and prior consultation obligations under Articles 32–36, including providing relevant information on the Service, subprocessors and safeguards. The Customer must give sufficient instructions and lawful authority for requested actions. Routine assistance is included; any exceptional, extensive work

requires a reasonable advance quotation and agreement, without obstructing statutory duties or charging for remediation of DPS's own breach.

D6 Information and audits

DPS must provide information necessary to demonstrate compliance with this schedule and allow and contribute to audits, including inspections, by the Customer or its mandated independent auditor. Documentation and remote review should be used first where adequate. Ordinarily audits take place on reasonable notice during business hours, with confidentiality and security arrangements that protect other clients. These arrangements must not prevent an audit required by law, a regulator or a substantiated incident.

The Customer may undertake one routine audit per year and additional audits justified by a material incident, reasonable compliance concern or regulator requirement. DPS may not refuse a necessary additional audit solely because a yearly limit has been reached. Each party normally bears its own audit costs; DPS bears its reasonable remediation costs where its breach is established. Audit scope must not expose unrelated client data, credentials or privileged information, but DPS must provide appropriate alternative evidence.

D7 Customer obligations

The Customer determines the lawful purposes and means of processing and is responsible for legal bases, notices, necessary permissions, accuracy, minimisation and retention instructions. It must ensure that any special category or criminal offence data processing is lawful and specifically documented. It must manage Authorised Users and securely configure disclosures, provide privacy and emergency contacts, and promptly notify DPS of any instruction change or concern. These obligations do not relieve DPS of its own processor duties.

Data locations and end of processing

D8 UK hosting and international access

Primary Customer content and production backups will be hosted in Microsoft Azure in the United Kingdom. DPS is established in Cyprus; authorised DPS personnel may access the Service from Cyprus for support and administration. UK hosting is a storage commitment and does not imply that identity, email or approved integration processing occurs only in the UK. All such providers, locations and relevant remote access must be identified in Schedule 4 before use.

DPS will not transfer or make Customer personal data accessible outside approved locations without a documented instruction and a lawful transfer mechanism where required. Transfers from the EEA to the UK may rely on an applicable EU adequacy decision while it remains effective. Transfers from the UK to Cyprus or another EEA country may rely on applicable UK adequacy regulations while effective. The parties must check the relevant scope and continued validity and not assume that UK hosting removes transfer obligations.

If adequacy is unavailable, DPS must put appropriate safeguards in place before continuing the restricted transfer, normally the applicable EU Standard Contractual Clauses and, for UK transfers, the UK International Data Transfer Agreement or approved UK Addendum as appropriate, with required assessments and supplementary measures. These transfer instruments must be completed and incorporated separately where needed; this schedule is not itself an international transfer instrument. If no lawful arrangement is possible, the affected processing must stop and the parties must agree an alternative or end the affected service.

DPS must review legally binding disclosure demands, challenge them where there are reasonable grounds, disclose only what is legally necessary and notify the Customer where legally permitted. It must not create voluntary access for public authorities or other recipients inconsistent with this agreement.

D9 Return and deletion

During the subscription the Customer may export records using the Service's available export functions. On expiry or termination, the Customer may choose return or deletion of its personal data. DPS will offer a standard electronic export of Customer Data, including available document files and structured records in a commonly usable format, through a secure channel. The Customer must communicate its choice within 30 days of the end date. This limited export period does not renew the subscription.

DPS will complete the requested standard return and delete active copies within that 30-day period, subject to agreeing a safe transfer where an export is requested near its end. If no instruction is received, DPS will notify the

Customer and delete active copies at the end of the period. DPS will confirm the export and deletion dates in writing. Customer Data must not be retained indefinitely because of unpaid fees.

Residual copies in backups will be isolated from ordinary use and removed through the backup lifecycle within 35 days after active deletion, and therefore ordinarily no later than 65 days after the service end date. If a backup is restored in that interval, DPS must reapply the deletion instruction before ordinary use. Any legally required retention must be limited to the relevant data and period, documented and disclosed where lawful, with continuing confidentiality and security. DPS must require equivalent return or deletion by subprocessors.

D10 Duration and continuing duties

This data agreement applies from the first processing of Customer personal data until all copies are returned or deleted in accordance with D9, including any legally required retention. Security, confidentiality, processor assistance and audit duties continue for retained data. Neither termination nor a liability clause changes either party's non-excludable obligations to regulators or data subjects.

Schedule 3 Processing details and security

P1 Description of processing

Subject matter: hosting, operating, maintaining and supporting the PIMS Workspace for the Customer. Purpose: privacy information management system and the Customer's related compliance programme under its documented instructions. Duration: the subscription and the limited return, deletion and legal retention periods in D9 and D10.

Operations: receiving and importing data, organising and storing it, displaying and retrieving it for authorised users, managing permissions, maintaining records and backups, authorised exporting and sharing, troubleshooting, restoring and deleting it. Optional AI or external integrations require the specific instructions and subprocessor entries described in D3 and section 5.5.

Typical workspace records: Privacy governance documents, processing inventories, assessments, privacy risks, incident and rights request records, supplier and contractual records, evidence, governance minutes and task assignments.

Data subjects: Customer users, employees, contractors, applicants where relevant, client and supplier contacts, auditors and individuals referenced in the Customer's compliance records. Types of personal data: names, business contact details, account identifiers, role and permission information, task and training records, access and audit logs, and personal data contained in Customer-supplied documents or records. The Customer must identify additional categories before uploading them.

Special category and criminal offence data: not required by default. The Customer must minimise such content, establish the necessary legal conditions and agree any additional safeguards in writing before processing it. No deliberate processing of children's data is included by default. Any additional data subjects, personal data categories, sensitive data, retention instructions and feature restrictions must be agreed in writing before the relevant processing begins.

P2 Minimum technical and organisational measures

Hosting and encryption. Store primary content and production backups in Azure UK. Apply AES-256 encryption at rest to production databases and backups, and equivalent protection to stored document content. Require HTTPS with TLS 1.2 or later for browser and service communications and encrypted, certificate-validated database connections. Manage secrets and encryption access through restricted systems, including Azure Key Vault where used; do not store secrets in shared documents or client-visible code.

Authentication and authorisation. Use individual identities with two-factor authentication. Enforce workspace membership and role permissions on the server, including for downloads, exports and record changes. Client administrators manage their own workspace; DPS administrative access across clients must be authorised and limited to legitimate duties. Auditors have appropriately restricted access and expiry. Revoke access when no longer needed and record relevant access and administrative changes.

Isolation and operations. Segregate clients' data and access, restrict production database connectivity and administrative interfaces, apply least privilege to service identities and restrict secrets. Maintain appropriate audit logs, monitor service and security events, manage vulnerabilities and apply updates. Control production changes, validate

releases and maintain incident response procedures. Do not expose another client's content through support, logs or exports.

Resilience and review. Maintain protected backups, the recovery commitments in Schedule 1 and documented restoration procedures. Test restoration and assess security measures periodically. DPS must assess any service-specific departure before commencement and agree replacement safeguards without reducing the contracted level of protection. These commitments do not imply that DPS or the workspace holds an ISO certification unless separately evidenced.

Schedule 4 Subprocessors

DPS must provide the approved subprocessor register before processing begins. It must identify the actual contracting legal entities, functions, locations and transfer safeguards, including relevant further subprocessors. A product brand alone is not a complete subprocessor disclosure. The Customer's general authorisation operates only as stated in D3.

Changes to this register follow D3. Customer-controlled systems to which the Customer directs an export must be identified as its authorised recipients, with roles and responsibilities clearly documented; they must not be silently treated as DPS subprocessors.