



Master Data Processing Agreement

Document Author	Roger Wallace
Document Owner	Karol Harkin
Status	Approved
Date Created	06-05-2026
Version	MDPA2
Last Updated	22-05-2026
Security Classification	Medium

Incorporation and Acceptance

This Master Data Processing Agreement (“**MDPA**”) is incorporated into and forms part of the Skylark Control Terms and Conditions of Use (“**Terms**”). By accepting the Terms — whether by account creation, platform access, or execution of an Order Form — the Customer agrees to be bound by this MDPA in respect of all personal data processed by the Company on the Customer’s behalf through the Skylark Platform.

This MDPA takes effect on the date the Customer accepts the Terms and remains in force for the duration of the Customer’s subscription. Where an enterprise customer has executed a countersigned Addendum with the Company, the Addendum takes precedence over this MDPA to the extent of any conflict.

The current version of this MDPA is published at
<https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>.

1. Definitions and Interpretation

In this MDPA, the following terms have the meanings set out below:

- “**Applicable Data Protection Law**” means the UK GDPR, the EU GDPR (where applicable to the processing of EU data subjects’ personal data), the Data Protection Act 2018, and any subordinate legislation or regulation made thereunder, as amended or replaced from time to time.
- “**APD**” means the Appropriate Policy Document maintained by the Company under DPA 2018 Schedule 1 Part 4, published at <https://admin.skylarkcontrol.com/legal/appropriate-policy.pdf> and updated from time to time.

- **“Automated Processing”** means the automated checking of worker certification and competency data against Customer-defined requirements within the Skylark Platform, producing decisions that affect whether a worker may accept or commence a work order.
- **“Business Day”** means any day other than a Saturday, Sunday, or public holiday in Northern Ireland, as further described in the Support Services Policy (SSP1).
- **“CDEP1”** means the Skylark Control Customer Data Retention & Erasure Policy, published at <https://admin.skylarkcontrol.com/legal/data-retention-policy.pdf> and updated from time to time, which governs the operational procedures for all customer data processed through the Skylark Platform.
- **“Company”** means Skylark Control Ltd, a company registered in Northern Ireland under company number NI651111, whose registered address is C/O Dnt Chartered Accountants Ormeau House, 91-97 Ormeau Road, Belfast, County Antrim, Northern Ireland, BT7 1SH.
- **“Customer”** means the organisation that has accepted the Terms and whose account details are registered with the Company.
- **“Customer Data”** means all personal data submitted to, generated within, or processed by the Skylark Platform by or on behalf of the Customer.
- **“Data Subject”** means the identified or identifiable natural person to whom personal data relates.
- **“Feature Activation”** means the act of enabling an optional platform feature — such as Asset Scheduling or Transfer of Control — through the platform’s feature activation workflow, which records the Customer’s acceptance against their account with a timestamp.
- **“Order Form”** means a written order for the Skylark Platform or specific platform features executed between the Company and the Customer, which may incorporate or supplement this MDPA.
- **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- **“Retention Register”** means the retention schedule set out in Section 12 of the CDEP1, which defines the applicable retention periods for each category of Customer Data.
- **“Security Policy”** means the Company’s Technical and Organisational Measures document, published at <https://admin.skylarkcontrol.com/legal/security-policy.html> and updated from time to time, which describes the security measures applied to Customer Data processed through the Skylark Platform.
- **“Skylark Platform”** means the software-as-a-service product provided by the Company under the Terms through which the Customer submits, manages, and processes data as part of its own business activities.
- **“Special Category Data”** means personal data falling within the categories defined by UK GDPR Article 9(1), including health data such as medical fitness certificates.
- **“Sub-processor”** means any third-party organisation engaged by the Company to process Customer Data on its behalf in connection with the delivery of the Skylark Platform.
- **“Sub-processor Register”** means the register maintained by the Company identifying each Sub-processor, the category of data they process, the purpose and nature of processing, and the geographic location(s) in which processing takes place, published at <https://admin.skylarkcontrol.com/legal/sub-processor-register.pdf> and updated from time to time.

All other capitalised terms used but not defined in this MDPA have the meanings given to them in the Terms or in Applicable Data Protection Law.

2. Subject Matter, Duration and Relationship of the Parties

2.1 Subject Matter

The Company processes Customer Data on behalf of the Customer in the course of delivering the Skylark Platform under the Terms. This MDPA governs all processing of personal data carried out by the Company as Data Processor acting on the Customer's instructions as Data Controller.

2.2 Duration

This MDPA takes effect on the date the Customer accepts the Terms and remains in force for the duration of the Customer's active subscription. Obligations relating to deletion, return, and record-keeping survive termination to the extent required by Applicable Data Protection Law and the CDEP1.

2.3 Relationship of the Parties

The Customer is the Data Controller in respect of Customer Data processed under this MDPA. The Company is the Data Processor. The Company does not determine the purposes or means of processing Customer Data and processes it solely on the Customer's documented instructions as set out in this MDPA, the Terms, and any applicable Order Form.

Different categories of Customer Data attract different roles for the Company, as set out in Schedule 1. Where the Company acts as Data Controller in respect of any category of Customer Data — for example, account and identity data processed to deliver and administer the service — that processing is governed by the CDEP1 and the Company's Privacy Notice, not by this MDPA.

3. Processing Details

3.1 Standard Processing

The categories of Customer Data, data subjects, nature and purpose of processing, and applicable retention periods for standard platform processing are set out in Schedule 1 Part A of this MDPA. By accepting the Terms, the Customer acknowledges that Schedule 1 Part A accurately describes the processing carried out by the Company in delivering the standard Skylark Platform service.

3.2 Special Category Data Processing

The collection of worker certificates, including health and fitness certificates, is a core platform capability available to all customers as part of the standard Skylark Platform service. Where those certificates constitute Special Category Data within the meaning of UK GDPR Article 9(1) — including medical fitness certificates — the additional warranties set out in Section 5 of this MDPA apply. By accepting this MDPA, the Customer confirms those warranties in respect of any Special Category Data it submits through the Platform. The processing of Special Category Data is described in Schedule 1 Part A.

3.3 Automated Processing

Automated Processing is a core platform capability available to all customers as part of the standard Skylark Platform service. It operates where the Customer has configured enforcement of worker certificates on their sites or work orders; it does not operate unless the Customer has made those configuration decisions within the Platform. The additional warranties set out in Section 5 of this MDPA apply where the Customer uses Automated Processing. By accepting this MDPA, the Customer confirms those warranties in respect of any use it makes of Automated Processing. The processing carried out in connection with Automated Processing is described in Schedule 1 Part A.

3.4 Customer Responsibility

The Customer is responsible for ensuring that its instructions to the Company comply with Applicable Data Protection Law at all times. The Customer undertakes to notify the Company promptly if any circumstances arise that affect the lawfulness of processing instructed under this MDPA, including any change to the lawful basis or Art. 9(2) condition applicable to Special Category Data processing.

4. Processor Obligations

4.1 Instructions

The Company will process Customer Data only on the documented instructions of the Customer as set out in this MDPA, the Terms, and any applicable Order Form, unless required to do otherwise by Applicable Data Protection Law. Where the Company is required by law to process Customer Data other than in accordance with the Customer's instructions, it will notify the Customer before processing unless prohibited from doing so by law.

4.2 Confidentiality

The Company will ensure that all persons authorised to process Customer Data are subject to a binding obligation of confidentiality in respect of that data, whether by contract or statutory duty.

4.3 Security

The Company will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with UK GDPR Article 32. A categorised summary of the current measures is set out in Annex 1 to this MDPA, and the full set of measures is described in the Security Policy published at <https://admin.skylarkcontrol.com/legal/security-policy.html>. The Security Policy is reviewed no less than annually. The Customer acknowledges that security measures may be updated from time to time in accordance with Section 16 of this MDPA, provided that any update does not materially reduce the level of protection afforded to Customer Data.

4.4 Sub-processors

The Company will not engage any Sub-processor to process Customer Data without prior authorisation in accordance with Section 6 of this MDPA. Where a Sub-processor is engaged, the Company will impose data protection obligations on that Sub-processor equivalent to those set out in this MDPA and will remain liable to the Customer for the Sub-processor's performance of those obligations.

4.5 Data Subject Rights

The Company will assist the Customer in responding to requests from data subjects exercising their rights under Applicable Data Protection Law, taking into account the nature of the processing and the information available to the Company. Where the Company receives a data subject rights request relating to Customer Data processed under this MDPA, it will notify the Customer within 5 working days of receipt and provide such assistance as is required by UK GDPR Article 28(3)(e) to enable the Customer to respond within the applicable statutory period.

4.6 Compliance Assistance

The Company will assist the Customer with its obligations under UK GDPR Articles 32 to 36, including in respect of security, Personal Data Breach notification, data protection impact assessments, and prior consultation with the Information Commissioner's Office, taking into account the nature of the processing and the information available to the Company.

4.7 Deletion and Return

Upon termination of the Customer's subscription or this MDPA, the Company will delete or return Customer Data in accordance with Section 13 of this MDPA, unless Applicable Data Protection Law requires retention beyond that point.

4.8 Audit and Information

The Company will make available to the Customer all information necessary to demonstrate compliance with the obligations in this Section 4 and will allow for and contribute to audits in accordance with Section 14 of this MDPA.

4.9 Cost of Assistance

Where the assistance reasonably required by the Customer under this Section 4, Section 10 (Personal Data Breach Notification), or Section 11 (Data Subject Rights) exceeds the assistance that the Company is obliged to provide under UK GDPR Article 28(3)(e) and (f) — taking into account the nature of processing and the information available to the Company — the Company may charge the Customer for the reasonable additional costs incurred. Where additional costs are anticipated, the Company will provide an estimate before incurring them where reasonably practicable, and will not unreasonably withhold the assistance pending agreement on those costs.

5. Customer Obligations and Warranties

The Customer warrants and undertakes that:

- It has established a valid lawful basis under UK GDPR Article 6 for each category of personal data processed under this MDPA, as described in Schedule 1 Part A
- The processing instructions given to the Company under this MDPA comply with Applicable Data Protection Law
- It will ensure that all data subjects whose personal data is submitted to the Skylark Platform have been provided with appropriate privacy information in accordance with UK GDPR Articles 13 and 14
- It will notify the Company promptly if any circumstances arise that affect the lawfulness of processing instructed under this MDPA

Where the Customer submits Special Category Data through the Platform, the Customer additionally warrants that:

- It has established a valid Art. 9(2) condition sufficient to authorise the processing of Special Category Data through the Skylark Platform and that this condition is documented in the Customer's own records
- It has maintained any Appropriate Policy Document required under DPA 2018 Schedule 1 Part 4 in respect of its own processing as Data Controller
- It will review the applicable Art. 9(2) condition no less than annually and will notify the Company if the condition changes or lapses

Where the Customer uses Automated Processing through the Platform, the Customer additionally warrants that:

- It is the Data Controller for all purposes of UK GDPR Articles 22A–22D in respect of automated decisions produced by the Skylark Platform affecting workers under its instructions
- It will ensure that all workers subject to Automated Processing are informed of its existence and nature, including the logic applied, the significance of decisions produced, and the envisaged consequences for workers, and will re-notify workers promptly where the configuration of Automated Processing changes materially
- It has provided workers with access to human review mechanisms through the Skylark Platform workflow, including certificate resubmission and manager approval capabilities, and accepts ongoing responsibility for ensuring workers can exercise those rights

6. Sub-processors

6.1 General Authorisation

By accepting this MDPA, the Customer grants general authorisation to the Company to engage the Sub-processors listed in the Sub-processor Register current at the date of acceptance. The Sub-processor Register is available to the Customer on request.

6.2 Changes to Sub-processors

The Company will notify the Customer of any intended addition or replacement of a Sub-processor no less than 30 days before the change takes effect. Notification will be given by email to the Customer's registered account email address and by update to the Sub-processor Register. The Customer may subscribe to Sub-processor Register change notifications through the Skylark Status page <https://status.skylarkcontrol.com>. The Customer has the right to object to a proposed change within 30 days of notification by notifying the Company in writing to privacy@skylarkcontrol.com. Where a Customer objects, the Parties will work together in good faith to resolve the objection before the change proceeds.

6.3 Special Category Data

Where the Customer submits Special Category Data through the Platform, the data processing agreement between the Company and any Sub-processor handling that data will explicitly identify Special Category Data as within scope of the processing. The Company will ensure that Sub-processors handling Special Category Data are bound by data protection obligations at least equivalent to those in this MDPA, and that access to Special Category

Data content is controlled exclusively by the Company through encryption and access management.

7. International Transfers

7.1 Transfer Restriction

The Company will not transfer Customer Data outside the United Kingdom or European Economic Area unless an appropriate transfer mechanism is in place, as identified in the Sub-processor Register, prior to the transfer commencing.

7.2 Transfer Mechanisms

Where a transfer outside the UK or EEA cannot be avoided, the applicable transfer mechanism will be one of: a UK adequacy regulation or EU adequacy decision (including, where applicable, the EU-US Data Privacy Framework (DPF) or the UK-US Data Bridge); an International Data Transfer Agreement (IDTA); or Standard Contractual Clauses (SCCs). Where the applicable mechanism is an IDTA or SCCs, a Transfer Impact Assessment will be completed and retained in accordance with the Retention Register before the transfer commences.

7.3 Sub-processor Transfers

Where a Sub-processor processes Customer Data outside the UK or EEA, the applicable transfer mechanism is identified in the Sub-processor Register. The Company will ensure that an appropriate mechanism is in place between the Company and the Sub-processor before processing commences.

7.4 EU Representative (Article 27 EU GDPR)

Where Customer Data processed under this MDPA falls within the territorial scope of EU GDPR Article 3(2), the Company has appointed an EU representative under Article 27 of the EU GDPR. EU-based data subjects and EU supervisory authorities may contact the EU representative on all matters relating to the processing of personal data:

- **EU Representative:** Data Protection Officer, Skylark Control Ltd
- **Email:** privacy@skylarkcontrol.com

The appointment of an EU representative does not affect the Company's own responsibility or liability under EU GDPR.

8. Special Category Data

This Section 8 applies where the Customer submits Special Category Data through the Platform.

- Acceptance of this MDPA constitutes the Customer's confirmation of the warranties set out in Section 5 in respect of any Special Category Data the Customer submits through the Platform. By submitting Special Category Data, the Customer affirms that those warranties are in place at the time of submission. The Company's record of the

version of this MDPA accepted by the Customer is retained as the record of those warranties.

- The Company confirms that it maintains an APD covering its processing of Special Category Data as Data Processor, published at <https://admin.skylarkcontrol.com/legal/appropriate-policy.pdf> in accordance with DPA 2018 Schedule 1 Part 4
- The Company will apply enhanced access controls, encryption, and the dedicated upload pathway classification mechanism described in the APD to all Special Category Data processed under this MDPA
- The Company's Data Protection Officer reviews account-level usage data no less than annually to identify customers submitting Special Category Data and to confirm that continued use remains within the scope of this MDPA. Where there is reason to believe the Customer's Art. 9(2) condition has lapsed or is invalid, the Company may suspend Special Category Data processing and will notify the Customer promptly
- Where Special Category Data processing is suspended under this Section, it will not resume until the Company is satisfied that a valid Art. 9(2) condition is in place

9. Automated Processing

This Section 9 applies where the Customer uses Automated Processing through the Platform.

- Acceptance of this MDPA constitutes the Customer's confirmation of the warranties set out in Section 5 in respect of any use the Customer makes of Automated Processing. By configuring certificate enforcement within the Platform, the Customer affirms that those warranties are in place at the time of configuration.
- The Company's role in Automated Processing is limited to the technical enforcement of certification and competency requirements as defined by the Customer, acting as Data Processor on the Customer's instructions
- The Company will not use Customer Data to train, test, or improve automated features or models within the Skylark Platform without the explicit written authorisation of the Customer

10. Personal Data Breach Notification

10.1 Company Notification Obligation

The Company will notify the Customer without undue delay and in any event by close of business on the Business Day following the day on which a Personal Data Breach involving Customer Data processed under this MDPA is confirmed. Notification will be sent to the Customer's registered account email address and will include, to the extent available at the time of notification:

- The nature of the breach, including the categories and approximate number of data subjects affected and the categories and approximate number of personal data records affected
- The name and contact details of the Company's Data Protection Officer or other contact point from whom further information can be obtained

- The likely consequences of the breach
- The measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

10.2 Special Category Data Breaches

Any breach involving Special Category Data, including medical fitness certificates, will be treated as high risk by default and escalated to the Company's Data Protection Officer immediately upon discovery, in accordance with the CDEP1.

10.3 Customer Cooperation

The Company will provide such reasonable assistance as the Customer requires to enable the Customer to meet its own notification obligations under UK GDPR Article 33 (ICO notification within 72 hours) and UK GDPR Article 34 (notification to affected data subjects where required).

11. Data Subject Rights

Where the Company receives a data subject rights request relating to Customer Data processed under this MDPA:

- The Company will acknowledge receipt and notify the Customer within 5 working days by email to the registered account email address
- The Company will direct the data subject to the Customer as the appropriate party to action the request
- The Company will provide such assistance as is required by UK GDPR Article 28(3)(e) within timeframes agreed with the Customer to enable the Customer to respond within the applicable statutory period
- The Company will not action a data subject rights request relating to Customer Data without the Customer's written instruction, except where required to do so by Applicable Data Protection Law

12. Retention Periods

Customer Data processed under this MDPA is retained in accordance with the Retention Register set out in Section 12 of the CDEP1. The Company will not retain Customer Data beyond the applicable period except where required to do so by Applicable Data Protection Law, or where an extended retention period has been authorised in writing by the Company's Data Protection Officer and recorded in the Company's Information Asset Register.

13. Termination and Deletion

13.1 Deletion Workflow

Upon termination of the Customer's subscription, the Company will:

1. Notify the Customer that their account has entered the deletion workflow
2. Provide the Customer with a period of 30 days to export any data they wish to retain before deletion commences
3. Initiate deletion of all Customer Data, including any Special Category Data, within 60 days of the termination date
4. Where the Customer has submitted Special Category Data, notify the Company's Data Protection Officer upon completion of primary deletion and obtain DPO sign-off before the Stage 1 confirmation in step 5 is issued
5. Issue a Stage 1 written confirmation to the Customer's registered account email address within 5 working days of primary deletion being completed, confirming that all Customer Data has been permanently deleted from primary systems and that backup purge will follow within 90 days
6. Once backup purge is complete (within 90 days of the primary deletion event), obtain DPO sign-off where the Customer has submitted Special Category Data, and issue a Stage 2 (final) written confirmation to the Customer's registered account email address confirming that all data has been permanently deleted across all systems including backups

13.2 Backup Systems

Customer Data held in backup systems will be purged within 90 days of the primary deletion event, in accordance with the backup rotation schedule described in the CDEP1.

13.3 Retained Data

Account, billing, and audit data will be retained for the periods specified in the Retention Register to satisfy the Company's legal and contractual obligations. The Company will not use retained data for any purpose other than that for which it is retained.

14. Audit Rights

14.1 Standard Assurance

The Company will make available to the Customer, on written request, its current third-party audit reports and security certifications relevant to the processing of Customer Data. Where those reports and certifications adequately address the Customer's compliance requirements, they satisfy the Company's audit obligations under this Section 14.

14.2 Direct Audit

Where the available certifications and reports do not fully address the Customer's compliance requirements, or following a confirmed Personal Data Breach involving the Customer's data, the Customer may request a direct audit of the Company's relevant systems and controls. Direct audits are subject to the following conditions:

- No more than one direct audit per 12-month period except following a confirmed Personal Data Breach
- A minimum of 30 days' written notice to privacy@skylarkcontrol.com, except following a confirmed Personal Data Breach where shorter notice may be agreed
- The audit is limited in scope to the Company's processing of Customer Data under this MDPA and compliance with the obligations set out herein

- The Customer bears its own costs in connection with a direct audit, except where the audit reveals a material breach by the Company, in which case the Company will bear the Customer's reasonable audit costs

14.3 Enterprise Customers

Enterprise customers with specific audit requirements may negotiate supplementary audit provisions through an Addendum in accordance with Section 18 of this MDPA.

15. Liability

Each Party's liability to the other under this MDPA is subject to the liability provisions set out in the Terms. Each Party will indemnify the other against any loss, damage, cost, or expense arising directly from a breach of its own obligations under this MDPA or Applicable Data Protection Law.

16. Updates to this MDPA

16.1 Company's Right to Update

The Company may update this MDPA, the Security Policy, the Sub-processor Register, and the APD from time to time to reflect changes in Applicable Data Protection Law, platform capabilities, or the Company's operational practices.

16.2 Material Updates

Where a proposed update to this MDPA materially affects the Customer's rights or obligations, the Company will provide no less than 30 days' written notice to the Customer's registered account email address before the update takes effect. Continued use of the Skylark Platform after the expiry of the notice period constitutes the Customer's acceptance of the updated MDPA.

16.3 Customer Objection

Where the Customer objects to a material update to this MDPA, the Customer may terminate its subscription on written notice given to legal@skylarkcontrol.com before the update takes effect, in accordance with the termination provisions of the Terms.

16.4 Non-material Updates

Updates to the Sub-processor Register, Security Policy, and APD that do not materially affect the Customer's rights or obligations take effect immediately upon publication. The Company will notify the Customer of such updates by email to the registered account email address.

17. Governing Law

This MDPA is governed by and construed in accordance with the law of Northern Ireland. Any dispute arising under or in connection with this MDPA is subject to the dispute resolution provisions set out in the Terms.

18. Enterprise Addendum

Enterprise customers who require bespoke data processing terms — including negotiated audit rights, specific deletion timeframes, or additional security commitments — may request a supplementary Addendum by contacting legal@skylarkcontrol.com. A countersigned Addendum takes precedence over this MDPA to the extent of any conflict. This MDPA continues to apply in all respects not addressed by the Addendum.

19. Notices

19.1 Notices to the Company

Notices required to be given to the Company under this MDPA — including objections to sub-processor changes (Section 6.2), audit notice (Section 14.2), termination on objection to a material update (Section 16.3), and Addendum requests (Section 18) — are to be given in writing to:

- **Privacy contact:** privacy@skylarkcontrol.com
- **Legal contact:** legal@skylarkcontrol.com
- **Postal address:** Skylark Control Ltd, 51, 55 High St, Antrim BT41 4AY

19.2 Notices to the Customer

Notices required to be given to the Customer under this MDPA — including notice of sub-processor changes (Section 6.2), Personal Data Breach notification (Section 10.1), data subject rights requests (Section 11), termination/deletion communications (Section 13), and material updates (Section 16.2) — are sent by email to the Customer's registered account email address recorded against the Customer's Skylark Platform account. The Customer is responsible for keeping that email address current and for ensuring that notifications sent to that address are monitored.

19.3 Deemed Receipt

A notice sent by email is deemed received at the time of transmission, provided the sender has not received a delivery failure notification. A notice sent by post is deemed received at the time it would have been delivered in the normal course of pre-paid first-class post.

20. General

20.1 Entire Agreement

This MDPA, together with the Terms and any countersigned Order Form or Addendum, constitutes the entire agreement between the Parties in respect of the processing of

Customer Data and supersedes all prior representations and understandings relating to the same subject matter.

20.2 Precedence

In the event of any conflict between this MDPA and the Terms, this MDPA takes precedence in respect of the processing of personal data. In the event of any conflict between this MDPA and a countersigned Addendum, the Addendum takes precedence.

20.3 Severability

If any provision of this MDPA is held to be invalid or unenforceable, the remaining provisions continue in full force and effect.

20.4 Survival

Sections 4 (Processor Obligations), 10 (Personal Data Breach Notification), 12 (Retention Periods), 13 (Termination and Deletion), 14 (Audit Rights), 15 (Liability) and this Section 20 survive termination of this MDPA to the extent required to give effect to their terms.

Schedule 1

Processing Details

Part A — Standard Processing

This Part A describes the processing carried out by the Company in delivering the standard Skylark Platform service. By accepting this MDPA, the Customer acknowledges that Part A accurately describes the processing carried out on its behalf. Part A is updated from time to time in accordance with Section 16.

Data Category	Categorie s of Data Subjects	Types of Personal Data	Nature of Processin g	Purpose	Com pany Role	Retenti on Period
Account and identity data	Platform users registered on behalf of the Customer	Name, email address, mobile number, organisation name, login credentials	Storage, access management	Platform delivery, user authentication, and account administration	Data Controller	Duration of contract + 6 years
Customer-submitted content	Workers, contractors, and	Documents, asset records,	Storage and retrieval on	Platform service delivery	Data Processor	Duration of contract

	other individuals whose data is submitted by the Customer	configurations, and any other data uploaded to or created within the platform	Customer instructions			+ 6 years
Worker certificates and competency records	Workers and contractors whose certification data is submitted by the Customer	Professional and trade competency certificates and safety training certificates	Storage and retrieval on Customer instructions	Supporting Customer's safe systems of work, statutory health and safety compliance, and workforce competency management	Data Processor	Duration of contract + 6 years
Medical fitness certificates	Workers and contractors whose health data is submitted by the Customer	Medical certificates of fitness to work	Storage and retrieval on Customer instructions	Supporting Customer's safe systems of work and statutory health and safety compliance	Data Processor	Duration of contract
Automated Processing	Workers assigned to work orders through the Platform	Certification records, competency records, work order assignment data	Automated cross-referencing of worker certifications against Customer-defined requirements, per site and work order configuration	Enforcement of Customer-defined certification requirements at point of work order assignment	Data Processor	Per Retention Register
Usage and behavioural data	Platform users	Work orders processed, session data, timestamps, audit trail entries generated	Storage, analysis	Service support, platform improvement, and security monitoring	Data Controller	12 months rolling

		by user actions				
Technical data — session and interaction	Platform users and customer integration accounts	IP addresses, device types, browser types	Storage, security monitoring	Service security and fraud prevention	Data Controller	12 months rolling
Technical data — API keys and integration credentials	Platform users and customer integration accounts	API keys, integration configuration data	Storage, access management	Service security and fraud prevention	Data Controller	Revoke d on contract end; records retained 1 year
Billing and commercial data	Customer billing contacts	Subscription details, payment records, contract-related information	Storage, financial administration	Contract management and legal obligation	Data Controller	6 years from date of transaction

Note: Where the Company acts as Data Controller for a category listed above, that processing is governed by the CDEP1 and the Company's Privacy Notice. Where the Company acts as Data Processor, processing is governed by this MDPA.

Note: Medical fitness certificates constitute Special Category Data under UK GDPR Article 9(1). The lawful basis for their processing is established by the Customer as Data Controller. By accepting this MDPA, the Customer confirms the warranties set out in Section 5 in respect of any Special Category Data it submits. See Section 8.

Note: Automated Processing operates where the Customer has configured certificate enforcement on their sites or work orders. The lawful basis for Automated Processing is established by the Customer as Data Controller. By accepting this MDPA, the Customer confirms the warranties set out in Section 5 in respect of any use it makes of Automated Processing. See Section 9.

Part B — Optional Feature Processing

This Part B describes processing carried out exclusively by optional platform features enabled through Feature Activation — such as Asset Scheduling and Transfer of Control. Where an optional feature involves processing of personal data not otherwise described in Part A, that processing is described here. Part B is updated from time to time in accordance with Section 16.

Data Category	Categories of Data Subjects	Types of Personal Data	Nature of Processing	Purpose	Company Role	Retention Period
---------------	-----------------------------	------------------------	----------------------	---------	--------------	------------------

Transfer of Control — authorisation records	Site Workers requesting work; Authorising Officers conducting the pre-commencement check	Worker identity and certification data (as described in Part A); Authorising Officer identity and role; transfer decision records	Display of worker data to the Authorising Officer for review; recording of authorisation decisions and Authorising Officer identity against the relevant work record	Supporting the customer's pre-commencement site access and safety check through the Transfer of Control feature	Data Processor	For duration of the contract
---	--	---	--	---	----------------	------------------------------

Note: "Authorising Officer" is a role specific to the Transfer of Control feature. Authorising Officers are platform users whose identity data is otherwise described under Account and identity data in Part A.

Annex 1

Technical and Organisational Measures

UK GDPR Article 32

This Annex is a categorised summary of the technical and organisational measures the Company has implemented in respect of the processing of Customer Data under this MDPA. The full set of measures is set out in the Security Policy (SECP1); where this Annex and the Security Policy address the same matter, the Security Policy provides the operational detail. The Company may update these measures from time to time in accordance with Section 16 of this MDPA, provided that any update does not materially reduce the level of protection afforded to Customer Data.

1. Physical and Site Access Control

The Skylark Platform operates entirely on cloud infrastructure; the Company maintains no on-premise server rooms or data centre facilities. The Company's office, used for administrative work on a hot-desking basis, has the following physical controls:

- Key-card access at the building entrance and at individual rooms
- CCTV monitoring at the building entrance
- Staffed front desk during Normal Business Hours
- No persistent storage of Customer Data on local Company devices

Sub-processors providing the underlying cloud infrastructure (DigitalOcean for primary hosting; AWS S3 for off-site backup) maintain their own physical access controls, certified to ISO 27001 and SOC 2 or equivalent.

2. System Access Control and Authentication

- Password-based authentication with mandatory multi-factor authentication (one-time code via email or SMS) for staff and customer administrator accounts
- Password complexity rules and a dictionary blacklist of compromised passwords applied at registration and password change
- Account lockout after 10 consecutive failed authentication attempts; unlock via documented account-recovery procedure with identity verification
- Login rate limiting at the authentication endpoint
- Session token expiry on inactivity (2 hours by default; configurable shorter by the Customer)
- Scoped API keys with least privilege, rate limiting, and request logging
- Passwords stored using BCrypt one-way hashing; plain-text secrets (passwords, API keys, MFA codes) are never transmitted or stored unencrypted

3. Authorisation and Access Management

- Role-Based Access Control with role assignments reviewed quarterly
- Privileged access reviewed quarterly
- Access permissions updated within 1 Business Day of any role change
- All access revoked within 4 hours of staff departure

4. Transmission Control (Encryption in Transit)

- TLS encryption applied to all inbound and outbound platform traffic
- TLS certificates issued and renewed automatically through Let's Encrypt on a 60-day cycle, with renewal-failure alerts to the operations team
- All data transfers between sub-processors and the Company are encrypted in transit and authenticated

5. Storage Control (Encryption at Rest)

- Customer Data encrypted at rest across DigitalOcean primary services (compute, managed databases, block storage, object storage) using the underlying platform encryption
- Off-site backups held in AWS S3 in the eu-west-2 (London) region, encrypted at rest using AES-256, with provider and data-centre separation from the DigitalOcean LON1 primary
- Copies of personal data are limited to backup and archive purposes; no separate operational copies are maintained
- Cryptographic erasure (permanent destruction of the encryption key) is the approved deletion method for Special Category Data and is subject to DPO sign-off

6. Input Control and Audit Logging

- All access to, and material changes affecting, Customer Data are recorded in the Company's audit logs
- Audit logs are retained for 5 years in accordance with Section 12 of the CDEP1

- Access logs recording access to and material changes affecting Customer Data are retained for 5 years in accordance with the Retention Register in Section 12 of the CDEP1
- Platform audit logs are retained for 1 year in accordance with the Retention Register in Section 12 of the CDEP1
- Logs supporting an active investigation, legal hold, or unresolved incident are retained beyond the standard period until the matter is closed

7. Separation and Multi-tenancy

- Customer Data is logically separated by tenant identifier within the platform
- Access controls enforce separation at the application layer
- Test, training, and development environments are isolated from production and do not contain Customer Data; where representative data is required for non-production use, synthetic or anonymised data is used

8. Availability and Resilience

- 99.9% monthly uptime target (excluding planned and emergency maintenance and force majeure)
- Platform configured for high availability with hot-standby instances and automated failover triggered by health-check failures
- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 5 minutes
- Nightly full backups with 10 days rotating retention, encrypted, off-site to AWS S3 in the eu-west-2 (London) region
- Point-in-time recovery for any point within the last 7 days through continuous transaction-log capture
- Disaster recovery plan tested no less than every 6 months

9. Vulnerability and Patch Management

- Vulnerabilities identified through cloud provider advisories, vendor bulletins, software composition analysis, and penetration testing
- Critical and High severity vulnerability remediation within 14 days; Medium within 30 days; Low within 90 days
- Critical operating system and application patches applied within 7 days of release
- Annual independent penetration testing by an accredited provider (current: Instil Software — NCSC-certified, Cyber Scheme Certified testers, ISO 27001 and ISO 9001 certified); scope covers web application, external network, mobile application (iOS and Android), API, and DigitalOcean VPC interior

10. File Upload Security

- All files uploaded by Customers to the Platform are scanned for malware before being made available
- Files containing executable scripting components — including scripted PDFs, macro-enabled office documents, and HTML or JavaScript payloads — are blocked at upload and not stored
- Customer-uploaded files are not executed server-side; uploaded files are stored for retrieval and download only

11. Incident Response

- Incidents logged in the Company's incident management system immediately on identification
- Initial triage within 2 hours of alert
- Customer notification of confirmed Personal Data Breach by close of business on the following Business Day (see Section 10)
- Post-incident review within 5 Business Days for Critical and High severity events
- Sub-processor incident notification to the Company within 24 hours

12. Personnel and Training

- Confidentiality obligations imposed on all personnel handling Customer Data, by contract and by statutory duty
- Security awareness training on joining and annually thereafter, delivered by Instil Software as Skylark's security partner; topics include data protection, phishing, password and authentication hygiene, and incident reporting
- Role-specific security training before access to production systems or Customer Data is granted
- Enhanced data protection training before access to Special Category Data is granted

13. Governance and Certification

- ISO 27001:2022 certified (transition completed 05-08-2025; full renewal audit 25-11-2025; next renewal 25-11-2026)
- Cyber Essentials Plus certification maintained
- Information Security Management System (ISMS) reviewed no less than annually
- ISMS risk assessment conducted no less than annually; risk register reviewed by senior management quarterly

Next review due: 08-05-2027

Document owner: Karol Harkin (Data Protection Officer) / Legal

Published at: <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>