



Customer Data Retention & Erasure Policy

Document Author	Paula McKinney, Roger Wallace
Document Owner	Karol Harkin
Status	Approved
Date Created	30 April 2026
Version	CDEP1
Last Updated	22 May 2026
Security Classification	Medium

1. Policy Statement

Skylark Control (*hereinafter referred to as the “**Company**”*) recognises its obligations in respect of the personal and confidential data it processes through the Skylark Platform on behalf of its customers. The Company is committed to managing customer data responsibly, transparently, and in full compliance with the **United Kingdom General Data Protection Regulation (UK GDPR)**, the **EU GDPR** and the **Data Protection Act 2018**.

This policy sets out the Company’s approach to the retention and erasure of customer data processed through the Skylark Platform. It is a companion document to the **Skylark Control Internal Data Retention & Erasure Policy (DREP-INT1)**, which governs the Company’s own operational records. Where both policies are relevant, each applies to its respective data category.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records and data management is necessary to:

- Fulfil the Company’s contractual obligations to customers in the delivery of the Skylark Platform
- Protect the rights and interests of the individuals whose personal data is processed through the platform
- Comply with data protection legislation, regulatory requirements, and contractual obligations

- Maintain the trust of customers by ensuring transparency and accountability in data handling
- Ensure that customer data is not retained beyond the period for which it is needed
- Provide customers with clear, actionable processes for exercising their data rights
- Support the Company's obligations as a Data Controller and/or Data Processor under UK GDPR
- Provide continuity in the event of a disaster or security breach
- Avoid inaccurate or misleading data and minimise risks to personal information

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The Company only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

2. Purpose

The purpose of this document is to define the Company's obligations and procedures for the retention, management, and erasure of data processed through the Skylark Platform. It establishes the standards by which customer data is collected, classified, stored, accessed, and deleted, and sets out the rights available to customers and the individuals whose data is processed.

This policy applies where the Company acts as a Data Controller in respect of customer data (for example, in respect of account and identity data processed to deliver the service), and where the Company acts as a Data Processor processing personal data on behalf of a customer controller.

3. Scope

This policy binds all staff within the Company involved in the delivery, support, or administration of the Skylark Platform in their handling of customer data (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

This policy covers Skylark Platform customer data only, meaning all data submitted to, generated within, or processed by the Skylark Platform by or on behalf of the Company's customers, including:

- Account and identity data of Skylark Platform users and all personal data processed by the Company in its capacity as a Data Processor on a customer's instructions
- Data submitted to the platform by customers in the course of using the service
- Usage and behavioural data generated by customer interactions with the platform
- Technical data generated by customer interactions with the platform
- Billing and commercial data associated with customer accounts

For the Company's own internal operational records, refer to the Skylark Control Internal Data Retention & Erasure Policy (DREP-INT1).

4. Customer Data on the Skylark Platform

The Skylark Platform is a software-as-a-service product through which customers submit, manage, and process data as part of their own business activities. This section defines the Company's obligations and approach in respect of that customer data.

The Skylark Platform collects and processes the following categories of customer data:

- **Account and identity data** — names, email addresses, mobile numbers, organisation names, and login credentials of individuals registered to use the platform on behalf of a customer organisation
- **Customer submitted content** — documents, asset records, configurations, relevant technical qualifications and medical certificates, and any other data that customers upload to or create within the platform in the course of using the service
- **Usage and behavioural data** — records of how customers interact with the platform, including work orders processed, session data, timestamps, and audit trail entries generated by user actions
- **Technical data** — IP addresses, device types, browser types, API keys, and integration configuration data
- **Billing and commercial data** — subscription details, payment records, and contract-related information associated with the customer account

4.1 Lawful Basis

Data Category	Lawful Basis	Skylark Control Role
Account and Identity Data	Performance of contract (Art. 6(1)(b))	Data Controller
Usage and Behavioural Data	Legitimate interests — service support, improvements and security (Art. 6(1)(f))	Data Controller
Customer-Submitted Content [1]	Customer's Art. 6 condition — see footnote [1] (Professional certificates and medical fitness certificates are covered as separate items in this table)	Data Processor
Technical Data	Legitimate interests — service support, security and fraud prevention (Art. 6(1)(f))	Data Controller
Billing and Commercial Data	Performance of contract and legal obligation (Art. 6(1)(b) and (c))	Data Controller
Professional certification and competency data (automated processing)	Customer's Art. 6 condition — see footnote [2]	Data Processor
Medical fitness certificates and associated automated processing	Customer's Art. 6 and Art. 9 conditions — see footnote [2]	Data Processor

[1] — Skylark processes customer-submitted content as a Data Processor acting on the instructions of the customer as Data Controller. The lawful basis for processing this data is established by the customer under their own applicable Art. 6 condition. Skylark does not rely on an independent lawful basis for this category; its authority to process derives from the obligations and instructions set out in the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>).

[2] — Skylark processes professional certification data and medical fitness certificates as a Data Processor. The customer acts as Data Controller for this processing, defining the certification requirements applied to work orders and managing certificate submission and approval through the Skylark Platform. Skylark enforces customer-defined requirements without discretion over the outcome and does not determine what constitutes a valid certificate.

The lawful basis for processing — including any applicable Art. 6 condition, any Art. 9(2) condition applicable to medical fitness certificates, and compliance with UK GDPR Articles 22A–22D in respect of automated decisions affecting workers — is the responsibility of the customer as Data Controller and must be confirmed in the Master Data Processing Agreement (MDPA) before processing commences. Skylark does not rely on an independent lawful basis or Art. 9 condition for this processing; its authority derives from the obligations and instructions set out in the Data Processing Agreement.

Skylark maintains appropriate technical and organisational safeguards for all special category data processed in its capacity as Data Processor.

4.2 Data Minimisation

The Skylark Platform is designed in accordance with the data minimisation principle under UK GDPR Article 5(1)(c). The Company only collects and processes customer data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Platform features are reviewed periodically to ensure that data collection does not exceed what is required for service delivery.

5. Objectives

A record is information, regardless of media; created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the Company's objective to implement the necessary records management procedures and systems which assess and manage the following processes:

- The collection, classification, and capture of customer data through the Skylark Platform
- Compliance with legal, regulatory, and contractual requirements applicable to customer data
- The secure storage of customer data throughout the contract lifecycle
- The protection of customer data integrity, authenticity, and confidentiality
- The controlled access to customer data by authorised personnel and users only
- The security of customer data in transit, at rest, and in backup systems

- The timely and verifiable deletion or export of customer data upon contract termination

Records contain information that are a unique and invaluable resource to the Company and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The Company's objectives and principles in relation to Data Retention are to:

- Retain customer data only for as long as is necessary to fulfil the purpose for which it was collected or to satisfy a legal or contractual obligation
- Provide customers with transparency about how their data is retained, managed, and deleted
- Ensure that data subjects are able to exercise their rights in respect of personal data for which the Company acts as Data Controller promptly and without undue restriction, and that where the Company acts as a Data Processor the customer controller is notified and supported in fulfilling any data subject rights request in accordance with the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>) and UK GDPR Article 28(3)(e)
- Comply with the relevant data protection regulation, legislation, and any contractual obligations including customer Data Processing Agreements
- Ensure the safe and secure disposal of customer data at the end of the retention period or upon a valid erasure request
- Maintain accurate records of all data processing activities, retention periods, and deletion events relating to customer data
- Mitigate against risks or breaches in relation to customer personal or confidential data
- Where special category health data, including medical fitness certificates, is processed through the Skylark Platform in connection with customers' safe systems of work and statutory health and safety obligations, ensure that such data is subject to enhanced protections commensurate with its sensitivity, processed solely on behalf of and under the instructions of the relevant customer as Data Controller, and retained only for as long as is necessary to fulfil the customer's contractual and legal obligations

6. Guidelines & Procedures

The Company manages customer data efficiently and systematically, in a manner consistent with the UK GDPR. Records management training inclusive of platform data handling obligations is mandatory for all Support, Platform operations and Product development staff as part of the Company's statutory and compliance training programme. Staff whose role involves access to, processing of, or decisions affecting special category data (including medical fitness certificates) must additionally complete enhanced data protection training covering the obligations applicable to special category data under UK GDPR Article 9 and DPA 2018 Schedule 1 Part 4. Completion of this enhanced training must be recorded and is a prerequisite for access to special category data within the Skylark Platform.

Customer data will be created, maintained, and retained in accordance with the terms of the applicable customer agreement and the retention schedules set out in the **Retention Register** at the end of this document.

It is our intention to ensure that all customer data and the information contained therein are:

- **Accurate** — customer data is processed as provided and records are maintained to reflect the current and historical state of the data accurately
- **Accessible** — customer data is made available to authorised customer users and authorised Company personnel only, with access controls maintained throughout the data lifecycle
- **Complete** — records of processing activities, retention periods, and deletion events are maintained to provide a full audit trail
- **Compliant** — all processing of customer data complies with UK Data Protection Act Schedule 1, the UK and EU GDPR, the applicable customer Data Processing Agreement, and any other relevant legal or regulatory requirements
- **Monitored** — compliance with this policy is regularly monitored and audited to ensure that the objectives and principles are upheld at all times

6.1 Retention Period Protocols

All customer data retained during its specified periods is traceable and retrievable. Any access to or movement of customer data is tracked and logged. Customer data is retained, stored, and deleted in line with legislative, regulatory, and contractual requirements.

For all customer data processed within the Skylark Platform, the Company:

- Carries out periodical reviews of retained customer data with specific checks on purpose, continued contractual validity, and requirement to retain
- Establishes and verifies retention periods for each data category, with consideration given to: the type and sensitivity of the personal data; the purpose and lawful basis of processing; and applicable statutory and regulatory retention requirements
- Where it is not possible to define a statutory or contractual retention period, the Company will identify the criteria by which the period can be determined and communicate this to the customer upon request
- Maintains processes to ensure that customer data subject to a legal hold, active investigation, or regulatory inquiry is not destroyed or altered until the hold is lifted

6.2 Designated Owners

All customer data categories and associated systems have designated owners (Information Asset Owners — IAOs) throughout their lifecycle to ensure accountability. Owners are assigned based on role and level of access required. The designated owner is recorded on the Retention Register. Skylark staff do not review, access, remove, or destroy customer data without the prior authorisation and knowledge of the designated Information Asset Owner. Where the data to be accessed or deleted is classified as Special Category under Section 6.3, the designated owner must additionally notify the Data Protection Officer and obtain DPO sign-off before access is granted or deletion is actioned.

6.3 Data Classification

Customer data processed through the Skylark Platform is assigned a classification in accordance with the Company's Information Asset Management protocols. All customer data classifications are recorded in the Information Asset Register (IAR) and reviewed as part of the Company's periodic Information Audits.

The Company utilises the following classification types for customer data:

- **Personal** — data that belongs to an individual and is classed as personal data under the data protection laws
- **Confidential** — customer data that must be secured at the highest level, afforded access restrictions, and protected by high user authentication
- **Special Category** — data falling within the categories defined by UK GDPR Article 9, subject to enhanced protections. The applicable Article 9 condition is established and documented by the customer as Data Controller and must be confirmed through the customer's acceptance of the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>). ***By accepting the MDPA, the customer warrants that it holds a valid Art. 9(2) condition before submitting any Special Category Data through the platform.*** Specifically: Medical certificates of fitness to work.

The Company's processing of special category data in its capacity as Data Processor requires the maintenance of an Appropriate Policy Document (APD) in accordance with DPA 2018 Schedule 1 Part 4. The APD must accurately reflect all special category processing activities conducted through the Skylark Platform. The currency and accuracy of the APD is reviewed no less than annually by the Data Protection Officer as part of the enhanced monitoring programme described in Section 9.

The classification assigned to customer data determines the access controls, security measures, and retention and deletion procedures applicable to that data.

6.4 Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information relating to customer data, or we are notified of the commencement of any litigation or regulatory investigation in which customer data is relevant, we will suspend the disposal of any scheduled customer data records until we are able to determine their relevance to the legal requirement. The customer will be notified of any such hold where the Company is legally permitted to do so.

A legal hold has the following effects for the duration of the hold:

- Scheduled deletion of the relevant data will not proceed. Where a deletion event would otherwise have been triggered — whether by retention period expiry, contract termination, or a data subject erasure request — it will be deferred until the hold is released or the data is confirmed as outside the scope of the legal requirement.
- The customer's right to export their data is not affected by the hold. Where the Company is legally permitted to notify the customer of the hold, the customer may request an export of the held data. Where notification is not permitted, export requests will be assessed on a case-by-case basis in accordance with the Company's legal obligations.

- The hold will be scoped as narrowly as possible to the data categories and records relevant to the legal requirement. Data outside the scope of the hold will continue to be processed and deleted in accordance with the normal retention schedule.
- When a legal hold is released — whether because the proceedings have concluded, the regulatory inquiry has closed, or the Company's legal advisers have confirmed that retention is no longer required — the Company will notify the customer in writing within 5 working days and resume the applicable retention and deletion schedule without undue delay.

6.5 Platform Data Lifecycle

Customer data processed through the Skylark Platform passes through the following lifecycle stages, each of which carries distinct obligations in respect of retention, access, and deletion:

- **Ingestion and Classification** — customer-submitted data is classified in accordance with Section 6.3 of this policy by virtue of the structured platform pathway through which it is submitted. Each data entry point and document type within the Skylark Platform maps to a defined data classification, ensuring that classification is applied consistently and automatically at the point of submission without reliance on Skylark staff review of individual records. Medical fitness certificates are classified as Special Category automatically, as the platform restricts their submission to a dedicated certificate upload pathway which applies Special Category classification and the associated access controls at the point of receipt. Platform-generated data (usage logs, audit trails) is automatically classified and tagged at the point of creation. All data is associated with the originating customer account to facilitate accurate retrieval and deletion.
- **Active Processing** — during an active contract, customer data is retained and processed in accordance with the terms of the customer agreement and the applicable retention periods set out in the Retention Register at the end of this document. Access is restricted to authorised personnel and to the customer's own authorised users as configured within the platform.
- **Account Suspension** — where a customer account is suspended but the contract has not been terminated, data is retained in full and access is restricted to read-only for a period not exceeding 90 days, unless otherwise agreed in writing. The customer retains the right to export their data during this period.
- **Contract Termination and Account Closure** — upon termination of a customer contract or closure of an account, the Company will:
 1. Notify the customer that their account has entered the deletion workflow
 2. Provide the customer a period of 30 days to export any data they wish to retain
 3. Initiate deletion of all customer-submitted content, including any special category data such as medical fitness certificates, within 60 days of the termination date
 4. Where special category data has been processed under the contract, notify the 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 within 5 working days of primary deletion being completed, confirming that all customer-submitted data has been permanently deleted from primary systems and that backup purge will follow within 90 days
 6. Retain account, billing, and audit data for the period specified in the Retention Register to satisfy legal and contractual obligations

7. Once backup purge is complete (within 90 days of the primary deletion event), obtain DPO sign-off where special category data was active, and issue a Stage 2 (final) written confirmation to the customer confirming that all data has been permanently deleted across all systems including backups
- **Backup and Archive Purge** — customer data, including special category data, held in backup systems will be purged in accordance with the backup rotation schedule, which is reviewed no less than annually. Backup purge will be completed within 90 days of the primary deletion event. Audit logs confirming deletion are retained for 5 years.

6.6 Third-Party Sub-processors

The Company uses third-party organisations to support the delivery of the Skylark Platform. Where those organisations process customer personal data on the Company's behalf, they are classified as sub-processors and are subject to the following requirements:

- The Company maintains a **Sub-processor Register** that identifies 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. This register is reviewed no less than annually.
- The Company conducts due diligence on all sub-processors prior to engagement and reviews their security and compliance posture periodically.
- Where possible, sub-processors operating in the UK or EU are chosen and international transfer of data is limited to the UK and EU countries. Where the sub-processor has data centres in multiple countries, an EU or UK option is selected. Where a transfer outside the UK or EEA cannot be avoided, an appropriate transfer mechanism must be confirmed prior to engagement — either an 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) — and where the mechanism is an IDTA or SCCs, a Transfer Impact Assessment completed and retained in accordance with the Retention Register (see Section 12).
- Where a data subject erasure request or other instruction requires deletion of data held by sub-processors, the obligation on each sub-processor is determined by its processing role:

Infrastructure sub-processors (DigitalOcean, AWS S3): All data is stored in environments under the direct operational control of the Company's IT function. Deletion is performed by the Company directly; the Company's own deletion records are the audit trail. No separate instruction to or confirmation from the sub-processor is required or meaningful.

Short-retention messaging sub-processors (transactional email and SMS): Both services auto-delete all processed data within 30 days of processing. In practice, data will have been purged within the standard DSR response window without any specific instruction being required.

- Sub-processors must ensure these obligations are flowed down to any further sub-contractors engaged in the processing of customer personal data.
- Where a sub-processor stores special category data on the Company's behalf, including medical fitness certificates, the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>) must explicitly identify that special category data is within scope of the processing. Access to stored special category data is controlled exclusively by the Company through encryption and access management; the sub-processor processes this data

as a storage provider acting solely on the Company's technical instructions and has no independent access to the data content.

- Upon termination of a customer contract, deletion obligations on sub-processors are determined by their processing role:

Infrastructure sub-processors (DigitalOcean, AWS S3): Deletion is performed directly by the Company's IT function using the Company's own administrative access. No sub-processor action is required; the Company's deletion records are the audit trail.

Short-retention messaging sub-processors (email and SMS): Both services auto-delete all processed data within 30 days of processing. No specific termination action is required; compliance is evidenced by their published retention terms, which are reviewed as part of the annual sub-processor review.

Any future sub-processor with independent data custody: Must delete all personal data held, including any copies, backups, or cached instances, within 60 days of the termination date, and must confirm deletion in writing to the Company.

7. Expiration of Retention Period

Once customer data has reached its designated retention period, the designated owner must refer to the Retention Register for the action to be taken. Where the data reaching expiry includes special category data, the designated owner must notify the Data Protection Officer and obtain DPO sign-off before deletion is actioned. Where data cannot be immediately deleted (for example, where it exists in backup systems), it will be flagged for purge at the next scheduled backup rotation.

Where retention beyond the primary period is required for legal or regulatory reasons, the Data Protection Officer must authorise the extension, document the legal or regulatory basis and a defined end date in the Information Asset Register, and review the extension no later than 12 months after the primary retention period expires. The extended retention period must not exceed the minimum period required by the identified legal or regulatory obligation. Where no statutory or regulatory period is prescribed, the extension must not exceed 3 years beyond the primary retention period without further DPO authorisation and Senior Management sign-off. The data will not be used for any other purpose during the extended period.

7.1 Destruction and Disposal of Records & Data

All customer data of a personal, confidential or special category nature held in electronic systems must be securely deleted when it is no longer required. The Company is committed to the secure and verifiable deletion of all customer data in accordance with its contractual and legal obligations.

The deletion of electronic customer data records must be organised in conjunction with the IT Function, who will ensure the removal of all data from the relevant system or medium so that it cannot be reconstructed. When a deletion event is triggered — whether by contract termination, retention period expiry, or a valid erasure request — the details must be recorded and provided to the designated owner to maintain an effective and up-to-date register of deleted records.

In all deletion instances, the IT Function must complete a deletion record and confirm successful removal of the data. Where the deletion relates to a customer account closure or contract termination, a written confirmation must be issued to the customer. Once deletion has occurred, the IT Function is responsible for liaising with the Information Asset Owner

and updating the Information Asset Register accordingly. Where the deletion event involves special category data, including medical fitness certificates, the IT Function must additionally notify the Data Protection Officer upon completion. The DPO must review the deletion record, confirm that deletion is complete across all storage environments including backups, and sign off the IAR update before the deletion event is considered closed.

8. Erasure

In specific circumstances, data subjects have the right to request that their personal data is erased. The Company recognises that this is not an absolute '*right to be forgotten*'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the Company receives a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with the relevant department manager and the IT team to ensure that all data relating to that individual is erased across all systems, including the Skylark Platform, backup systems, and any data shared with sub-processors.

For platform customers, the erasure workflow in Section 6.5 (Platform Data Lifecycle — Contract Termination and Account Closure) applies in full where a customer organisation requests deletion of its account data, in addition to the standard DPO-led process for individual data subject erasure requests.

Where we receive a request to erase and/or remove personal information from a data subject, the process below is followed:

- The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
- The DPO uses the Information Asset Register (IAR) and data mapping records to locate all personal information relating to the data subject held across the Company's systems, including the Skylark Platform, backup systems, and any data held by sub-processors, and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
- The request is reviewed to ensure it complies with one or more of the grounds for erasure:

The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed

The data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing

The data subject objects to the processing and there are no overriding legitimate grounds for the processing

The personal data has been unlawfully processed

The personal data must be erased for compliance with a legal obligation

The personal data has been collected in relation to the offer of information society services to a child

- Where the erasure request relates to special category data, including medical fitness certificates, the DPO must carry out a safety obligation assessment before proceeding. This assessment must confirm: whether the data currently underpins a live automated access decision or an active safety obligation of the relevant customer; and whether the relevant customer controller has confirmed that no active contractual or statutory obligation is dependent on the data
- Where personal data must be retained to comply with a legal obligation, including obligations under the Health and Safety at Work etc. Act 1974 and associated regulations, the Company may refuse or restrict a request for erasure in accordance with Article 17(3)(b) of the GDPR
- If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
- The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
- Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links, and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

Such refusals to erase data include:

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

8.1 Special Category Data

In accordance with UK GDPR (*tailored by Schedule 1 Part 4 of The Data Protection Act 2018*), organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

In supporting customers' Safe Systems of Work, Skylark receives and processes Medical Certificates on behalf of customer Data Controllers. Details of the automated processing of

these and other professional certificates are covered in the Section on Automated Processing and Profiling.

8.2 Automated Processing and Profiling

The Skylark Platform provides automated processing capabilities that customers configure and deploy as part of their own compliance obligations. Where such automated processing produces decisions with legal or similarly significant effects on individual workers, compliance with UK GDPR Articles 22A–22D is the responsibility of the customer as Data Controller.

Skylark's obligations as Data Processor in support of those requirements are to:

- Clearly identify and document all automated processing capabilities operating within the platform in the Information Asset Register, and make this information available to customers
- Provide customers with the technical capability to inform their workers of any automated processing that significantly affects them, including the logic, significance, and envisaged consequences
- Provide the technical mechanisms through which workers may exercise their rights in respect of automated decisions, including certificate resubmission, manager approval workflows, and human review requests, as described below
- Ensure that customer data is not used to train, test, or improve automated features or models without explicit customer authorisation
- Where customer-submitted data is used to train, test, or improve automated features or models within the platform, this will be clearly disclosed and, where required, subject to a separate consent or contractual provision. Customer data will not be used for such purposes without explicit authorisation.

The Skylark Platform enforces certification and competency requirements on behalf of customers. The automated checking logic operates as follows:

- **Logic:** The system cross-references a worker's approved certifications and competencies against the requirements configured for a specific work order by the customer.
- **Consequence:** If a worker does not hold a current approved certification meeting the customer's configured requirements, the system will automatically prevent them from accepting or starting that work order.
- **Responsibility:** The customer acts as Data Controller for this processing. The customer defines the certification requirements, manages the certificate submission and approval workflow, and is responsible for compliance with UK GDPR Articles 22A–22D in respect of automated decisions affecting their workers. Skylark acts as Data Processor, providing the technical enforcement mechanism on the customer's instructions.
- **Worker recourse:** Workers who believe a certification decision is incorrect should use the certificate resubmission workflow within the Skylark Platform. Managers may approve or resubmit certificates on a worker's behalf. The customer is responsible for ensuring workers are informed of automated decisions and have access to human review through the platform workflow.

8.3 Data Subject Rights for Platform Customers

Platform customers and the individuals whose data is processed through the Skylark Platform retain all rights afforded to data subjects under the UK GDPR. The Company is committed to facilitating the exercise of these rights promptly and without undue restriction.

Where a data subject rights request relates to data processed by the Company in its capacity as a Data Processor acting on a customer's instructions, such as customer-submitted content held on the Skylark Platform, the request cannot be actioned by the Company directly. In such cases the Company will:

- Acknowledge receipt of the request and notify the relevant customer controller within 5 working days
- Direct the data subject to the customer controller as the appropriate party to action the request
- Provide such assistance to the customer controller as is required by the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>) and UK GDPR Article 28(3)(e)

The rights and processes described in this section apply where the Company acts as a Data Controller in respect of the relevant data, as set out in Section 4.1 of this policy.

The following rights apply and are actioned within the timeframes specified:

- **Right of Access (Subject Access Request — SAR)** — individuals have the right to obtain confirmation of whether their personal data is processed, and to receive a copy of that data together with supplementary information. The Company will respond to all SARs within **30 days** of receipt. This period may be extended by a further 60 days where requests are complex or numerous, provided the individual is notified within the initial 30-day period.
- **Right to Rectification** — individuals have the right to have inaccurate personal data corrected and incomplete data completed without undue delay. Customers may update account data directly within the platform; other rectification requests should be directed to the Data Protection Officer. Where a rectification request relates to professional certification or medical fitness certificate data, workers and their managers may submit, approve, or resubmit certificates directly through the Skylark Platform. Rectification of certification data is managed by the customer through the platform workflow.
- **Right to Erasure** — as set out in Section 8 of this policy. For platform customers, the erasure workflow in this document applies in full in addition to the standard DPO-led process.
- **Right to Restriction of Processing** — individuals have the right to request that the processing of their personal data is restricted where: the accuracy of the data is contested; the processing is unlawful but the individual opposes erasure; the Company no longer needs the data but the individual requires it for legal claims; or the individual has objected to processing pending verification of legitimate grounds. During a restriction, the Company will only store the data and will not process it further without consent or for legal claims.
- **Right to Data Portability** — where Skylark acts as a Data Controller and processing is based on consent or contract and is carried out by automated means, individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller. The Skylark Platform supports data export in CSV or Excel format to facilitate the exercise of this

right. Portability requests will be fulfilled within 30 days. This right does not apply to data processed by Skylark in its capacity as a Data Processor on a customer's instructions; in such cases the data subject should direct their request to the relevant customer controller.

- **Right to Object** — individuals have the right to object to processing based on legitimate interests or for direct marketing purposes. Where an objection is received in respect of direct marketing, processing will cease immediately. Where an objection is received in respect of legitimate interests processing, the Company will assess whether compelling legitimate grounds exist that override the interests of the data subject.

All data subject rights requests received in connection with the Skylark Platform should be submitted to the Data Protection Officer and will be logged on the Data Subject Rights Register. The Company will respond in writing confirming the action taken or, where a request is refused, providing the reasons for refusal and informing the individual of their right to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy.

8.4 Identity Verification

Before actioning any data subject rights request, the Company will take proportionate steps to verify the identity of the requester. Verification is applied to protect data subjects against unauthorised disclosure and is not used as a barrier to the exercise of rights. The response clock does not begin until identity has been verified.

Requests from Site Owners and Site Delegates

Site Owner contact details are mandatory at the point of account creation and are held on the customer account record. Where a request is received from a claimed Site Owner, identity is verified by matching the request against the registered contact details for that account. Where a Site Owner has designated one or more Site Delegates, delegate contact details are held on the account record and the same verification approach applies.

Where a request relates to customer-submitted data processed by the Company in its capacity as a Data Processor, the Company will not take action on that data without the knowledge and consent of the registered Site Owner or a Site Delegate, who are the appropriate Data Controller contacts for that data.

Requests from Individual Platform Users

Where a request is received from an individual who accesses the Skylark Platform as a worker or contractor, the Company will verify identity using the contact details held for that individual on the platform:

- **Primary verification:** the email address and mobile number registered to the individual's platform account. A request originating from a registered email address or confirmed by a one-time verification to the registered mobile number satisfies primary verification.
- **Secondary verification:** where primary verification is not possible because the registered email address or mobile number is no longer valid or accessible, the Company will contact the individual's employer to confirm their identity and current contact details.

For individuals employed directly by a Site Owner customer, the Company will contact the registered Site Owner or Site Delegate.

For individuals employed by a third-party contractor, the Company will contact the registered Contract Manager. Identity is confirmed once the employer contact provides written confirmation that the individual is or was employed by them.

Requests from Third Parties Acting on Behalf of a Data Subject

Where a request is received from an agent or representative acting on behalf of a data subject — including a legal representative or family member — the Company will require written evidence of the authority to act, such as a signed letter of authority or power of attorney, before processing the request. The identity of the agent is verified against the authority document. The identity of the data subject is verified using the methods described above where possible.

Where Verification Cannot Be Completed

Where the Company is unable to verify the identity of a requester, the request will be suspended and the requester notified in writing within 5 working days, setting out what information is needed to complete verification. If identity cannot be established within 30 days of the verification notice being sent, the Company will close the request and notify the requester in writing that the request cannot be progressed. The requester will be informed of their right to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy. The outcome will be recorded on the Data Subject Rights Register.

9. Compliance and Monitoring

The Company is committed to ensuring continued compliance with this policy and any associated legislation, contractual obligations, and regulatory requirements. Regular audits and monitoring of customer data processing activities, retention practices, and deletion events are undertaken. Information Asset Owners (IAO) are tasked with ensuring the continued compliance and review of customer data within their remit.

The Company will conduct a formal review of this policy no less than annually, or following any material change to the Skylark Platform, applicable law, or customer contractual requirements.

Escalation and Remediation

Where non-compliance with this policy is identified — whether through audit, monitoring, a data subject rights request, or any other means — the following process applies:

- The IAO for the affected data must notify the Data Protection Officer (DPO) without undue delay upon identifying or being made aware of the non-compliance.
- The DPO will assess the nature and severity of the non-compliance and escalate to the relevant Head of Department and, where the matter involves a potential breach of data protection legislation or significant risk to data subjects, to Senior Management.
- A documented remediation plan must be produced by the relevant IAO within 10 working days of the non-compliance being confirmed. The plan must identify the corrective actions required, the responsible party, and a target completion date.
- The DPO will verify completion of the remediation plan and record the outcome. Where non-compliance involves wilful or repeated breach of this policy, the Company's disciplinary procedures, as referenced in Section 3, may be invoked.

Personal Data Breach Notification

Where a monitoring or audit activity reveals, or gives reasonable grounds to suspect, a personal data breach involving customer data processed through the Skylark Platform, the Company will comply with its obligations under UK GDPR Article 33 and, where EU data subjects are affected, EU GDPR Article 33:

- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Company will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Where notification cannot be made within 72 hours, the notification will include a reasoned explanation for the delay.
- The Company's obligation to notify customers of a confirmed Personal Data Breach (by close of business on the Business Day following confirmation, as required by the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>)) runs concurrently with the ICO 72-hour notification obligation. Customer notification is set well in advance of the ICO deadline to allow customers sufficient time to prepare their own Art. 33 notification where required.
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, affected data subjects will be notified without undue delay in accordance with UK GDPR Article 34.
- All personal data breaches will be recorded in the Company's Security Incident register, in Plane (<https://plane.so>), regardless of whether ICO notification is required.
- Any breach involving special category data, including medical fitness certificates, will be treated as high risk by default and escalated to the DPO immediately upon discovery.
- Further detail on breach identification, triage, and response, including the severity classification framework and the Personal Data Breach notification assessment, is set out in Section 9 of the Security Policy (SECP1 — <https://admin.skylarkcontrol.com/legal/security-policy.html>).

Special Category Data — Enhanced Monitoring

In addition to the standard audit and monitoring programme, the Company applies the following enhanced monitoring checks to special category data processed through the Skylark Platform. These checks are conducted no less than annually and are recorded by the DPO:

- **APD currency:** confirmation that the Appropriate Policy Document required under DPA 2018 Schedule 1 Part 4 remains current and accurately reflects all special category processing activities on the platform.
- **Art. 9 condition review:** confirmation that for each customer who has submitted Special Category Data through the Skylark Platform under the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>), the customer's applicable Art. 9(2) condition has been reviewed within the monitoring period. Where there is reason to believe a customer's Art. 9(2) condition has lapsed or is invalid, that processing must be suspended until the Company is satisfied that a valid condition is in place.
- **Access control verification:** confirmation that access to special category data, including medical fitness certificates, is restricted to authorised personnel, that access logs have been reviewed for the period under review, and that no anomalous access events have occurred without documented justification.

- **Sub-processor compliance:** verification that sub-processors handling special category data continue to meet their obligations under the Master Data Processing Agreement and that their security and compliance posture has been reviewed within the monitoring period.
- **Retention schedule adherence:** confirmation that medical fitness certificates and other special category data are being deleted in accordance with the retention periods specified in Section 12, with deletion records reviewed and signed off by the DPO.

10. Responsibilities

Heads of departments and Information Asset Owners have overall responsibility for the management of customer data generated by or within their areas of responsibility, namely to ensure that data is processed, retained, and deleted in a way which meets the aims of this policy and the requirements of the applicable customer Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>).

The Data Protection Officer (DPO) must be involved in all non-routine customer data retention and erasure decisions. This includes: authorising extensions to retention periods; signing off deletion of special category data; reviewing and actioning data subject erasure requests; and any retention or deletion decision that falls outside the schedules and procedures established in this policy. Routine deletions executed in accordance with the Retention Register — including automated log purges, scheduled backup rotations, and standard account closure workflows — do not require individual DPO sign-off, provided they are carried out in accordance with this policy and the deletion event is recorded. Records of all deletion events must be maintained in the Information Asset Register.

The IT Function is responsible for the technical execution of all deletion and purge events, maintaining access controls over customer data throughout its lifecycle, completing deletion records, and updating the Information Asset Register upon deletion. The IT Function acts on written instructions from the designated IAO, or the DPO as applicable.

The Customer Success function is responsible for managing customer-facing communications relating to data retention and deletion, including account closure notifications, export window coordination, and written deletion confirmations issued to customers.

The Finance function is responsible for ensuring that billing, invoice, and payment records are retained and disposed of in accordance with the Retention Register and applicable tax and accounting obligations.

Individual employees must ensure that customer data for which they are responsible is handled in strict accordance with the Company's protocols and the applicable customer agreement.

11. Retention Periods

Section 12 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1*).

Note that where a user account is associated with an active organisational subscription, individual user inactivity shall not trigger data deletion. Records shall be retained for the duration of the organisational contract plus 90 days, or as otherwise agreed in the Master Data Processing Agreement (MDPA — <https://admin.skylarkcontrol.com/legal/master-data-processing-agreement.pdf>).

Section 12

Retention Register

Record	Retention Period	Asset Officer	Action	Notes
Customer account data (name, email, organisation, login credentials)	Duration of contract + 6 years	IT / DPO	Delete / Anonymise	Retained post-contract to satisfy legal and contractual obligations; anonymised after 6 years where archiving is required
Platform usage and behavioural logs	12 months rolling	IT	Delete	Logs older than 12 months are purged automatically; retained beyond this only where required for an active investigation or legal hold
Customer-submitted content (documents, records, configurations)	Duration of contract + 6 years	IT / DPO	Delete on expiry or on customer request	30-day export window provided to customers upon account closure before deletion commences; see Section 6.5
Customer Submitted Medical Certificates of fitness to work	Duration of contract	IT / DPO	Delete on expiry or on customer request	30-day export window provided to customers upon account closure before deletion commences; see Section 6.5
Platform audit logs	1 year	IT	Delete	Auto-purged after 1 year; retained beyond this only where required for an active investigation or legal hold
Access logs	5 years	IT	Archive then delete	Deleted on schedule; retained beyond this only where required for an active investigation or legal hold

Deletion audit logs	5 years	IT / DPO	Archive then delete	Records of deletion events confirming secure disposal of customer data, per 6.5
Customer support and helpdesk records	3 years from ticket closure	Customer Success / DPO	Delete	Includes support tickets, email correspondence, and call records relating to platform issues
API access tokens and integration credentials	Revoke immediately on contract end; records retained 1 year	IT	Revoke and delete	Token records retained for 1 year post-revocation to support incident investigation
Billing, invoice, and payment records	6 years from date of transaction	Finance	Archive then delete	Required for tax and accounting obligations
Master Data Processing Agreement (MDPA) — acceptance records, Order Forms, and supplementary Addenda	Duration of contract + 6 years	Legal / DPO	Archive then delete	Retained to evidence compliance with processing obligations
Sub-processor agreements and due diligence records	Duration of relationship + 6 years	Legal / DPO	Archive then delete	
Data subject rights requests (SARs, erasure, portability)	3 years from date of response	DPO	Archive then delete	Retained to demonstrate compliance with response obligations
Transfer impact assessments (TIAs)	Duration of transfer arrangement + 3 years	DPO	Archive then review	Review triggered if destination country laws change materially
Consent records (where processing based on consent)	Duration of consent + 3 years after withdrawal or expiry	DPO	Delete	Records must demonstrate what consent was given, when, and on what basis

Document owner: Karol Harkin (Data Protection Officer)

Version: CDEP1 | Last updated: 22 May 2026