



Appropriate Policy Document

Special Category Data — DPA 2018 Schedule 1 Part 4

Document Author	Roger Wallace
Document Owner	Karol Harkin
Status	Approved
Date Created	06-05-2026
Version	APD1
Last Updated	22-05-2026
Security Classification	Medium

1. Purpose and Scope

This Appropriate Policy Document (APD) is maintained by Skylark Control in accordance with the Data Protection Act 2018 Schedule 1 Part 4. It documents the Company's policies and procedures for the processing, retention, and erasure of special category personal data processed through the Skylark Platform.

This APD covers processing carried out by Skylark Control in its capacity as a Data Processor acting on the instructions of customer Data Controllers. It is a companion document to the Skylark Control Customer Data Retention & Erasure Policy (CDEP1), which governs the operational procedures for all customer data processed through the platform. Where this APD and the CDEP1 address the same matter, the CDEP1 provides the operational detail; this document provides the Schedule 1 Part 4 compliance record.

This APD must be made available to the Information Commissioner's Office on request.

2. Special Category Data in Scope

The following special category data is processed through the Skylark Platform:

Data Type	Art. 9 Category	Processing Nature
Medical fitness certificates	Health data (Art. 9(1))	Storage and automated processing on customer instructions

Medical fitness certificates are submitted by or on behalf of workers to customers using the Skylark Platform in connection with customers' Safe Systems of Work and statutory health and safety obligations under the Health and Safety at Work etc. Act 1974 and associated regulations.

No other special category data is currently processed through the Skylark Platform. This document will be updated if additional categories are introduced.

3. Processing Role and Art. 9 Condition

3.1 Skylark's Role

Skylark Control acts as a Data Processor in respect of all special category data processed through the Skylark Platform. The customer organisation acts as Data Controller, defining the processing purposes and instructions under which Skylark operates.

Skylark does not determine the purpose or lawful basis for processing special category data and does not rely on an independent Art. 9 condition. Its authority to process derives solely from the obligations and instructions set out in the Master Data Processing Agreement (MDPA).

3.2 Art. 9 Condition

The applicable Art. 9(2) condition depends on the nature of the customer's workforce and processing purpose. Customers may rely on one or more of the following conditions:

- **Art. 9(2)(b)** — processing necessary for obligations and rights in the field of employment law (DPA 2018 Schedule 1 Part 1). Appropriate for directly employed workers.
- **Art. 9(2)(h)** — processing for preventive or occupational medicine. May apply where processing supports a customer's Safe Systems of Work under the Health and Safety at Work etc. Act 1974.
- **Art. 9(2)(a)** — explicit consent of the data subject. May apply where the worker is self-employed or the employment relationship is absent or attenuated.

The applicable condition is held and relied upon by the customer as Data Controller, who is responsible for identifying the correct condition having regard to their workforce composition. Before any special category processing commences under a customer contract, the customer's applicable Art. 9(2) condition must be confirmed through the customer's acceptance of the Master Data Processing Agreement (MDPA). 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. Where the Company has reason to believe that a customer's Art. 9(2) condition has lapsed or is invalid, special category processing will be suspended until the Company is satisfied that a valid condition is in place.

3.3 Necessity of Processing

Processing of medical fitness certificates is necessary to enable customers to operate automated certification and competency checking as part of their Safe Systems of Work. The Skylark Platform enforces customer-defined certification requirements at the point of work order assignment. Without processing this data, the platform cannot support the customer's statutory health and safety compliance obligations.

4. Purposes of Processing

Special category data processed through the Skylark Platform is used solely for the following purposes, as defined by the customer as Data Controller through the Master Data Processing Agreement (MDPA):

- Storage of medical fitness certificates submitted by or on behalf of workers
- Automated checking of certificate validity against customer-defined requirements at the point of work order assignment
- Facilitating human review and resubmission workflows where an automated decision is contested

Special category data is not used for any purpose beyond those defined in the MDPA. Customer data is not used to train, test, or improve platform features or models without explicit customer authorisation.

5. Retention Policies

5.1 Standard Retention Period

Medical fitness certificates are retained for the duration of the customer contract only. Upon contract termination, deletion is initiated within 60 days in accordance with the termination workflow set out in Section 6.5 of the CDEP1.

The full retention schedule for medical fitness certificates is set out in the Retention Register at Section 12 of the CDEP1.

5.2 Extended Retention

Where retention beyond the primary contract 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.

5.3 Compliance with Retention Periods

The following procedures ensure that retention periods for special category data are complied with:

- The Retention Register (CDEP1 Section 12) records the applicable retention period for medical fitness certificates
- Information Asset Owners are responsible for identifying data approaching the end of its retention period
- The DPO must be notified and must sign off all special category data deletion events before they are actioned
- The enhanced monitoring programme (CDEP1 Section 9) includes an annual retention schedule adherence check conducted by the DPO

- Deletion records are maintained in the Information Asset Register

6. Erasure Procedures

Requests for erasure of special category data are handled in accordance with Section 8 of the CDEP1. The following procedures apply specifically to special category data:

- Before any erasure of medical fitness certificates is actioned, the DPO must carry out a safety obligation assessment confirming that the data does not currently underpin a live automated access decision or active safety obligation of the relevant customer
- Where data must be retained to comply with a legal obligation, including obligations under the Health and Safety at Work etc. Act 1974, the Company may refuse or restrict erasure in accordance with Art. 17(3)(b) UK GDPR
- Where erasure is confirmed, deletion is carried out within 30 days of the request being received
- The DPO must sign off completion of deletion before the erasure event is recorded as closed in the Information Asset Register

7. Technical and Organisational Safeguards

The following safeguards are applied to all special category data processed through the Skylark Platform. The full set of technical and organisational measures is described in the Skylark Control Security Policy (SECP1), published at <https://admin.skylarkcontrol.com/legal/security-policy.html>. This section records the measures specific to special category data:

- **Classification at ingestion** — medical fitness certificates are classified as Special Category automatically at the point of submission by virtue of the dedicated certificate upload pathway within the platform, which applies Special Category classification and associated access controls without reliance on manual review.
- **Access controls** — access to special category data is restricted to authorised personnel only. Skylark staff do not access special category data without the prior sign-off of the designated Information Asset Owner and the Data Protection Officer.
- **Encryption** — special category data is encrypted at rest and in transit. Cryptographic erasure — permanent destruction of the encryption key — is the approved deletion method for cloud-hosted special category data.
- **Sub-processor controls** — primary processing and storage of special category data takes place on the DigitalOcean platform; off-site backup copies are held in AWS S3 acting as a storage-only sub-processor. The applicable data processing agreements with DigitalOcean and AWS explicitly identify special category data as within scope. Neither sub-processor has independent access to the data content; access is controlled exclusively by Skylark through encryption and access management.
- **Backup purge** — special category data held in backup systems is purged within 90 days of the primary deletion event, in accordance with the backup rotation schedule.

8. Staff Training

All staff whose role involves access to, processing of, or decisions affecting special category data must 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 before access is granted. Completion of this training is recorded and is a prerequisite for access to special category data within the Skylark Platform.

9. Monitoring and Review of this Document

This APD is reviewed no less than annually by the Data Protection Officer. Review is also triggered by any material change to:

- The categories of special category data processed through the Skylark Platform
- The technical or organisational safeguards applied to that data
- The applicable law or regulatory guidance
- Any material change to the Master Data Processing Agreement (MDPA)

The annual review is recorded as part of the enhanced monitoring programme set out in Section 9 of the CDEP1. Where this APD is found to be inaccurate or out of date, it must be updated before the monitoring record is signed off by the DPO.

This APD is maintained for as long as special category data processing continues through the Skylark Platform and for a minimum of 6 months after all such processing has ceased. The six-month post-cessation period is a policy commitment, not a statutory requirement.

Document owner: Karol Harkin (Data Protection Officer)

Version: APD1 | Last updated: 22-05-2026