Ref.	261910001 / 10.05.2026
To:	To Whom It May Concern
Subject:	Information Notice Regarding Data Storage, Backup and Cybersecurity Policy for the eCMSMS and eFTLMon Applications

Dear Madam/Sir,

This letter is issued to provide general information regarding the data storage, backup and cybersecurity policy applicable to the eCMSMS and eFTLMon applications.

The eCMSMS application is designed to support organizations in the management of compliance, safety reporting, information security reporting, actions/CAPA, meetings, documents, training, SMS/ERP, ISMS/IRP and Management of Change processes, depending on the acquired package and configuration.

The eFTLMon application is designed to support organizations in the management of crew rostering and FTL monitoring.

1. Data Storage

Data entered in the eCMSMS and eFTLMon applications is stored in a controlled digital environment and is used exclusively for the purpose of operating the application and supporting the organization's internal management processes.

The stored data may include, depending on the modules used:

- user account information;
- organizational roles and access rights;
- audit records and compliance findings;
- safety reports and related follow-up actions;
- information security reports, where applicable;
- CAPA/action records;
- meeting minutes and related actions;
- document records and controlled files;
- training and qualification records;
- risk registers, performance indicators, ERP/IRP records and MoC records, where applicable;
- system logs and traceability records.

Access to stored data is managed through user authentication and role-based access control. Users are granted access only to the areas and functions required for their assigned responsibilities.

2. Data Access and Confidentiality

The application is intended to ensure controlled access to information based on user roles, permissions and organizational responsibilities.

Administrative access is restricted to authorized personnel only. Any access performed for support, maintenance or troubleshooting purposes is limited to what is necessary for the proper operation of the application.

The data remains the property and responsibility of the customer organization. eCMSMS and eFTLMon do not use customer data for unrelated purposes, commercial resale, advertising, profiling or disclosure to unauthorized third parties.

3. Backup Policy

The application is operated with a backup process intended to reduce the risk of data loss and to support recovery in case of technical failure or accidental data unavailability.

The backup policy may include:

- periodic database backups;
- periodic backup of uploaded files and documents;
- retention of backup copies for a defined period;
- storage of backups in a controlled environment;
- restoration support in case of system incident, technical failure or data recovery request.

The exact backup frequency, retention period and recovery arrangements may be defined in the applicable service agreement, hosting agreement or customer-specific implementation documentation.

Unless otherwise agreed, backups are intended for disaster recovery and operational continuity purposes and are not a substitute for customer-side export, archiving or records management obligations.

4. Cybersecurity Measures

The eCMSMS and eFTLMon applications are developed and operated with cybersecurity controls intended to protect the confidentiality, integrity and availability of stored information.

Cybersecurity measures include:

- user authentication;
- role-based access control;
- separation of permissions by user group and responsibility;
- controlled administrative access;
- server-side access restrictions;
- database access restrictions;
- activity logs and system traceability;
- secure handling of uploaded files;
- regular maintenance and updates;
- technical controls to reduce unauthorized access risk;
- backup and recovery arrangements;
- monitoring of relevant operational or security issues, where applicable.

5. Data Retention

Data is retained for the duration of the customer's use of the application, unless otherwise agreed contractually or required by applicable regulatory, legal or organizational requirements.

Upon termination of the service, data export, retention or deletion arrangements should be agreed between the parties, taking into account applicable contractual obligations, regulatory recordkeeping requirements and operational needs.

6. Customer Responsibilities

The customer organization remains responsible for:

- assigning appropriate user roles and permissions;
- ensuring that only authorized personnel receive access;
- maintaining confidentiality of user credentials;
- defining internal data retention requirements;
- reviewing exported records and reports;
- ensuring that use of the application aligns with applicable legal, regulatory and organizational requirements;
- promptly notifying the service provider of any suspected unauthorized access, data issue or cybersecurity concern.

7. Deployment-Specific Arrangements

The data storage location, backup frequency, retention period, cybersecurity controls and service-level commitments are provided as hosted Software-as-a-Service application.

8. Statement of Intent

The eCMSMS and eFTLMon applications are intended to provide a structured, controlled and traceable digital environment for compliance, safety, information security, management system and FTL related activities.

The application's data storage, backup and cybersecurity arrangements are designed to support secure operation, operational continuity and auditability, while maintaining customer control over organizational data and access rights.

Should further technical details be required, a dedicated technical annex or security questionnaire response may be provided upon request.

Yours faithfully,

Mihail VOICU
Administrator
SafeWings Aviation Consulting SRL