



LANDING.AERO / RESEARCH & PRACTICAL GUIDANCE

EU Occurrence Reporting: Data Handoff and Follow-Up Evidence

LANDING.AERO is a Montreal software studio that builds custom, AI-assisted software for flight operations: operations tools, data integration, workflow automation and dashboards designed around how an airline, charter operator or flight department actually works.

Published by LANDING.AERO · 2026-10-20 · eu occurrence reporting · regulation 376/2014 · eccairs · e5x · mandatory occurrence reporting · 72 hours occurrence reporting · just culture · safety management system · aviation safety reporting · easa

Original article: <https://www.landing.aero/articles/en/eu-occurrence-reporting-data-handoff-evidence>



In this article

1. Executive Summary
 2. Introduction and Background
 3. Key Changes and Requirements Under the Current Framework
 4. The Evidence-Event Contract
 5. Formats, Taxonomy and Authority Channels
 6. Implementation Considerations and Process Changes
 7. Data Analysis and Evidence
 8. Implications and Future Directions
 9. Frequently Asked Questions (FAQs)
 10. Conclusion
-

Executive Summary

EU occurrence reporting for aviation is governed by Regulation (EU) No **376/2014**, and its timing rules are narrower and more conditional than the phrase "all events within 72 hours" suggests. Individuals in the listed roles must report to their organisation "within 72 hours of becoming aware of the occurrence, unless exceptional circumstances prevent this" (eur-lex.europa.eu). The organisation, after notification, reports to its competent authority "as soon as possible, and in any event no later than 72 hours after becoming aware" (eur-lex.europa.eu). Follow-up is a separate, conditional duty: where analysis identifies an actual or potential safety risk, preliminary results and any action go to the authority "within 30 days from the date of notification of the occurrence by the reporter", and final results are due in principle within **three months** (eur-lex.europa.eu).

The practical difficulty is that "becoming aware" is not a database field. EASA guidance says that for automated data collection the 72-hour period starts when the person responsible for analysing the data detects the reportable occurrence (easa.europa.eu), and the Commission guidance says a retrospective report restarts the organisation's count on receipt (www.easa.europa.eu). Air Operations rule **ORO.GEN.160(d)** words its own trigger differently, as the operator "identifying the condition to which the report relates" (eur-lex.europa.eu). A single dashboard clock cannot show which actor knew what and when. This report therefore proposes an evidence-event contract: a ledger of awareness, classification, submission, receipt and correction events, each with a UTC timestamp, a named human role and an access class.

Identity protection shapes the design. Each organisation must designate one or more persons to handle reports independently and safeguard the confidentiality of reporter identity (www.easa.europa.eu), no personal details may ever be recorded in the national database, and Commission guidance encourages organisations to omit names when transferring reports to the authority (www.easa.europa.eu). Format and channel are partly national: the Regulation requires ECCAIRS and ADREP compatible formats (eur-lex.europa.eu), but Germany's Federal Aviation Office (LBA) states that its ECCAIRS 2 portal has been the only permitted reporting route since 15 February 2023 (www.lba.de), while Sweden documents an API with a receiving-authority identifier (www.transportstyrelsen.se).

Revisions matter. Commission Implementing Regulation (EU) **2026/1821** replaces the annexes of the mandatory occurrence list from **17 August 2026** (eur-lex.europa.eu), while EASA's easy-access edition of Regulation 376/2014 is dated 19 December 2022 (www.easa.europa.eu). Scale is material: the European Central Repository (ECR) held **2,548,578** reports at the end of 2019, the latest total in the Commission's 2020 report, and later sections give more recent figures from other sources (eur-lex.europa.eu), and Ireland's aviation authority records **13,439** reports from its AOC holders in 2024 (www.iaa.ie). This report is analysis, not legal advice, and does not replace an operator's approved procedures or the instructions of its competent authority.

Introduction and Background

This report addresses European air operator certificate (AOC) safety managers and the IT or data leads who either select an occurrence-reporting platform or connect an internal safety management system (SMS) intake to a competent-authority submission system. The jurisdiction is the European Union. The framework is Regulation (EU) No 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation, supplemented by Implementing Regulation (EU) 2015/1018 (the mandatory lists), Delegated Regulation (EU) 2020/2034 (the risk classification scheme) and, for operators, the Air Operations Regulation (EU) No 965/2012. It does not apply to United States Part 135 or Part 121 operations, which sit under a different legal system. Together, organisation-level reporting systems, national databases and the European Central Repository form the EU aviation safety occurrence reporting system that this report examines.

The Regulation defines an occurrence as "any safety-related event which endangers or which, if not corrected or addressed" could endanger an aircraft, its occupants or any other person (www.easa.europa.eu). It defines an organisation as one providing aviation products or employing, contracting or using the services of persons required to report. Each such organisation must establish a mandatory reporting system (www.easa.europa.eu), and the Basic Regulation (EU) 2018/1139 independently requires an air operator's management system to include an occurrence reporting system that complies with Union law.

Three terms need care throughout:

- **Reporter notification:** when a person tells the organisation.
- **Organisation awareness:** when the organisation is deemed to know.
- **Authority submission:** sending data to the competent authority, which is distinct from authority receipt and from onward transfer to the ECR.

The Regulation uses these ideas in different places, and an evidence design that collapses them into one timestamp loses the information an auditor, a just-culture review or a data-quality check will need.

A note on sources. The Regulation text quoted here comes from EASA's easy-access edition, which EASA itself describes as not an official publication, and from the EUR-Lex pages that could be opened during research. As of October 2026 the EASA edition is dated 19 December 2022, and a consolidated EUR-Lex version should be checked before any design is frozen. Nothing here is legal advice; the distinction between a legal requirement and an implementation example is flagged wherever it matters.

Key Changes and Requirements Under the Current Framework

Scope, actors and independent handling

Regulation 376/2014 assigns duties to three tiers. Listed individuals report first through the system of the organisation that employs, contracts or uses their services (www.easa.europa.eu). The organisation runs its mandatory reporting system and a voluntary system, and the text allows the two to be integrated into a single system. Competent authorities hold national databases, and the Commission manages the European Central Repository. For operators, ORO.GEN.160 adds that reports go to the competent authority and to any other organisation the State of the operator requires to be informed.

Article 6(1) is the provision most relevant to platform design. Each organisation must designate one or more persons to handle independently the collection, evaluation, processing, analysis and storage of reported details. EASA's guidance on reporting-system compliance advises the same designation and notes that this will usually be the safety or quality department. Recital 34 adds that a clear separation between the departments handling occurrence reports and the rest of the organisation may limit the transmission of personal details. For software, this implies a role model in which the handling persons are named, not generic "administrators".

Voluntary reports follow a looser path. The Regulation requires an organisation's voluntary reports to be forwarded to the competent authority "in a timely manner" rather than within a fixed number of hours. An integrated intake must therefore carry a mandatory or voluntary flag, because the downstream clocks differ.

The reportability decision and the 2026 list revision

Whether an event is mandatorily reportable is decided against lists. Implementing Regulation 2015/1018 states that the detailed classification "is set out in Annexes I to V" (eur-lex.europa.eu), and its original Annex I is headed "occurrences related to the operation of the aircraft". The annex remarks make clear that the activity headings are presentational and do not mean an occurrence outside the heading need not be reported. The lists are not a ceiling: EASA guidance in the easy-access book notes that occurrences may be reported if judged relevant by potential reporters, so an event absent from the list can still be reported.

The lists changed in 2026. EASA's page for Commission Implementing Regulation (EU) 2026/1821 describes it as the act "laying down a list classifying occurrences in civil aviation to be mandatorily reported" (www.easa.europa.eu). EUR-Lex lists the act as adding unmanned aircraft system, U-space and Part-IS occurrences and removing certain aviation security occurrences from mandatory reporting, with a date of effect of **17 August 2026** (eur-lex.europa.eu). The retrieved material did not include the new annex text, so an operator should map its internal event taxonomy to the current consolidated list and treat any mapping built against the 2015 annexes as needing review.

Two further classification steps follow. First, Article 7(2) requires reports to include a safety risk classification, reviewed and endorsed by the competent authority or EASA. The Delegated Regulation sets out the common European risk classification scheme (ERCS) (eur-lex.europa.eu), which "shall address the safety risk of an occurrence and not its actual outcome" (eur-lex.europa.eu) and has applied since 1 January 2021. Second, the operator's own classification (for example a severity and likelihood matrix inside its SMS) is a separate, internal judgement and should be stored as a separate field from the ERCS value.

Timing: what the clocks actually are

Table 1 below summarises the timing provisions that matter to an operator, with the trigger of each. The point of the table is the trigger column: the same figure of 72 hours attaches to two different actors and, in ORO.GEN.160, to a differently worded trigger.

Rule	Who acts, to whom	Trigger and limit	Basis
Individual report	Listed person to own organisation	Within 72 hours of becoming aware, unless exceptional circumstances prevent this	Art 4(7)
Organisation report	Organisation to competent authority (or to EASA for EASA-certified organisations)	As soon as possible, no later than 72 hours after becoming aware	Art 4(8), 4(9)
Operator report	Air operator to competent authority and design organisation	As soon as practicable and within 72 hours of the operator identifying the condition	ORO.GEN.160(d), Reg 965/2012
Preliminary analysis	Organisation to competent authority	Only where analysis identifies an actual or potential risk: within 30 days of reporter notification	Art 13(4), 13(5)
Final analysis	Organisation to competent authority	As soon as available, in principle no later than three months from notification	Art 13(4), 13(5)
National database to ECR	Competent authority	No later than 30 days after entry in the national database (eur-lex.europa.eu)	Art 9(1)

The table shows that the operator's evidence obligations are front-loaded around two start events (awareness and reporter notification), while the later rows are authority-side deadlines the operator cannot control but may need to explain. The Commission's 2021 evaluation records industry stakeholder comments on the 30-day preliminary-analysis timeline (edz.bib.uni-mannheim.de), which is a reason to log the reason whenever follow-up is late or inapplicable.

Guidance also fixes some start points for awkward cases. For automated systems such as flight data monitoring, the Commission guidance says the 72 hours start when the potential reporter is made aware of the occurrence, and EASA's FAQ says the period starts when the person responsible for the analysis of the data detects it. Where an organisation asked for a retrospective report, its count starts when it receives that report.

Conditional preliminary and final follow-up

Article 13 requires each organisation to develop a process to analyse the occurrences it collects. The transmission duty is conditional: only where that analysis identifies an actual or potential aviation safety risk must the organisation send the competent authority its preliminary results and any action to be taken, within 30 days of the reporter's notification. Final results follow as soon as available and in principle within three months. The words "if any" and "in principle" are why the evidence design needs an explicit "no actual or potential risk identified" decision event, owned by a named person, so that the absence of a follow-up submission is itself traceable.

For operators, ORO.GEN.160(e) separately asks for a follow-up report on the actions the operator intends to take, "as soon as these actions have been identified" (eur-lex.europa.eu), in the form and manner set by the competent authority. This is a different trigger from Article 13 and carries no 30-day figure. Because two follow-up provisions coexist, a ledger should record which provision a given submission answers.

Finally, EASA's data-quality guidance lists "checking consistency between initial reports and any follow up reports about an occurrence", and Article 7(3) requires data quality checking processes (www.easa.europa.eu). A follow-up that silently overwrites the initial report would defeat this check, which is why correction events are versioned in the contract below.

Just culture, identities and personal data

The Regulation defines just culture as one in which front-line operators are not punished for actions, omissions or decisions commensurate with their experience and training, while gross negligence, wilful violations and destructive acts are not tolerated. Article 16(11) requires each organisation, after consulting staff representatives, to adopt internal rules describing how just-culture principles are guaranteed (www.easa.europa.eu). Employees who report or are mentioned in reports must not suffer prejudice from their employer on that basis, subject to the exceptions in Article 16(10), which include a manifest, severe and serious disregard of an obvious risk (www.easa.europa.eu).

The data rules are concrete. Personal details may reach staff other than the designated persons only where absolutely necessary to investigate, and disidentified information is disseminated within the organisation as appropriate. "Disidentified" means personal data such as names or addresses have been removed. The Commission guidance notes that the Regulation does not require organisations to fully anonymise the reports they collect, but encourages them to refrain from including names and personal details when transferring reports to the authority. Information from reports may be used only for the purpose for which it was collected, and the guidance states that disclosure to judicial authorities is not allowed except in limited cases.

The GDPR bridge is indirect. The Regulation text still refers to the former data protection directive, and GDPR Article 94(2) provides that such references are construed as references to the GDPR (eur-lex.europa.eu). The Commission's 2021 evaluation observed that disidentified information can still contain personal data, so compliance must still be ensured (edz.bib.uni-mannheim.de), and that personal data occasionally reaches the central repository because of human error (edz.bib.uni-mannheim.de). That finding is a reasonable design input for pre-submission checks.

The Evidence-Event Contract

Why a dashboard clock is not evidence

A countdown timer answers "how long since the record was created". It does not answer which actor became aware, whether the reportable decision was reviewed by the designated person, which authority received which version, or whether the follow-up reached the authority. Vendor documentation illustrates the gap in a neutral way: one provider states that its solution "keeps a 72-hour clock for the submission of MORs"

(mandatory occurrence reports) (www.ideagen.com). That is a vendor claim about a feature, and the legal question of when the clock legitimately started remains one of fact and procedure, as the guidance above shows.

The contract below is an implementation example, not a legal requirement. It rests on two legal anchors: ORO.GEN.220 requires a record-keeping system allowing "adequate storage and reliable traceability of all activities" (www.easa.europa.eu), and the associated AMC says computer systems should include safeguards against unauthorised alteration of the data.

The ledger

Table 2 lists the events that should be separately traceable. Each row names a source system, a timestamp rule, a human role, an access class (P for protected identity, R for restricted safety-handling, G for general SMS users), the regulatory basis, the evidence or receipt expected, and an exception path.

Event	Source and timestamp	Responsible role	Access class	Basis	Evidence or receipt	Exception path
1. Detection	Source system (crew report, FDM tool, maintenance system); UTC with offset recorded	System owner for automated sources	G	Guidance: automated detection is not automatically "awareness"	Raw detection record, hash or immutable ID	Late-arriving data flagged with ingestion time
2. Reporter notification	Intake form or API; UTC	Reporter (identity held under P)	P	Art 4(6), 4(7)	Intake ID, reporter reference	Retrospective report requested: new event type
3. Organisation awareness	Designated-person action; UTC	Named designated person	R	Art 4(8)	Signed action in audit log	Awareness disputed: both candidate times retained
4. Reportability decision	Review form; UTC	Named designated person, with second reviewer for "not reportable"	R	Art 4 and 2015/1018 lists	Decision, list reference version	Borderline: escalate to safety manager; record rationale
5. Classification	Internal matrix and ERCS fields; UTC	Safety manager	R	Art 7(2)	Internal score, ERCS value, authority endorsement later	"Pending" status allowed but tracked
6. Disidentification	Transform step; UTC	Designated person	P to R	Art 15, 16(2)	Before/after field list, no names in outbound payload	Free-text scrub failure: block submission

Event	Source and timestamp	Responsible role	Access class	Basis	Evidence or receipt	Exception path
7. Authority submission	Outbound message; UTC	Named submitter	R	Art 4(8); ORO.GEN.160(d)	Payload hash, version number, channel, target authority	Channel down: documented fallback route
8. Authority receipt	Portal or API response; UTC	System, reviewed by submitter	R	Portal behaviour, not a statutory receipt rule	Acknowledgement message, reference number	No acknowledgement: re-query or escalate
9. Correction or update	New version; UTC	Designated person	R	Art 7(3)	Version chain linking to prior payload	Authority returns report for edit (www.transport.gov.mt)
10. Follow-up decision	Analysis record; UTC	Safety manager	R	Art 13(1), 13(4)	Risk identified: yes or no, with rationale	Not applicable: recorded "no risk identified"
11. Preliminary and final analysis submission	Outbound message; UTC	Safety manager	R	Art 13(4)	Payload, receipt, due-date calculation	Late: reason code, new expected date

The table is deliberately more granular than most SMS dashboards. Rows 3, 4 and 10 are decisions by humans and are the ones an audit will test; rows 7 and 8 are machine events and should never be inferred from each other. The table also carries a "second reviewer" suggestion that is a design choice, not a legal rule.

The design principles behind the ledger can be stated briefly:

- **Separate events:** detection, notification, awareness, decision, submission and receipt are never merged into one field.
- **Named humans:** every decision event carries a named role holder, not a team alias.
- **Immutable history:** corrections add versions; they never overwrite earlier entries.
- **Access classes:** protected identity data sits in a different class from safety-handling data and from general SMS views.
- **Receipts as received:** channel responses are stored unaltered, with the time they arrived.
- **Exceptions explicit:** late, not-applicable and failed-channel cases have reason codes rather than blank fields.

Timestamps, time zones and versions

The common mandatory fields in Annex I include "UTC Date" in the "When" group, and the ECCAIRS coding guidance warns that this attribute (ID 477) "should not be confused with" the local date of occurrence attribute (aviationreporting.eu). The same guidance sets the UTC date format as DD/MM/YYYY (aviationreporting.eu).

The E5X implementation note for organisations also lists a "Reporting date" attribute, defined as the date the report was sent to the authority (aviationreporting.eu). The contract therefore stores every event in UTC with the source offset retained, and keeps the occurrence date, the awareness time and the submission time as three independent values.

Versioning follows from the submission mechanics. Sweden's technical documentation, for example, recommends always using **MINOR** as the version type for API submissions (www.transportstyrelsen.se). Whatever the national channel, the ledger should hold the payload exactly as sent for each version, with a link to the version it supersedes.

Illustrative calculation (Hypothetical Example)

This calculation is not a legal clock. It shows what a ledger can compute once events are separate. All times are UTC, on a fictional occurrence.

- **Reporter notification:** 2026-03-03 08:14.
- **Organisation awareness recorded by the designated person:** 2026-03-03 09:02.
- **Reportability decision:** 2026-03-03 14:40.
- **Authority acknowledgement of submission:** 2026-03-04 16:06.

Elapsed time from recorded organisation awareness to acknowledgement is **31 hours 04 minutes**. Measured from reporter notification the figure is **31 hours 52 minutes**. The 48-minute difference is exactly the ambiguity that a single timer hides. If the occurrence had instead been detected by an automated system at 2026-03-02 22:00 and the analyst detected it at 2026-03-03 07:30, EASA's FAQ wording would point to the analyst's detection as the start, which is why both system and human timestamps are stored. For Article 13, 30 days from reporter notification on 2026-03-03 is 2026-04-02, and three months is 2026-06-03, both conditional on a risk being identified.

Formats, Taxonomy and Authority Channels

ECCAIRS, ADREP and E5X

Article 7(4) requires organisation, national and EASA databases to use formats compatible with the ECCAIRS software and the ADREP taxonomy. The Commission guidance lists the E5X file format as one acceptable means and describes it as mostly meant for large organisations producing many reports a month (www.easa.europa.eu). EASA states that E5X is the IT route for organisations to transfer data from their Annex 19 database to a competent authority's ECCAIRS environment. The E5X note explains that files can be created from IT environments without requiring an ECCAIRS installation (aviationreporting.eu), and the format is XSD-based so data can be formally validated before submission (aviationreporting.eu).

The content is a subset of the taxonomy: the Reduced Interface Taxonomy (RIT) contains a little over **280** data fields (aviationreporting.eu). EASA treats E5X files as valid if they adhere to the latest ECCAIRS taxonomy, and the portal's taxonomy page lists change packages between versions v5112 and v5100 (aviationreporting.eu). The current taxonomy release as of October 2026 could not be confirmed from the

readable pages, so the taxonomy version used by a connector must be checked with the receiving authority. The 2015 implementation note also proposed limiting attachments inside an E5X file to under 10 MB (aviationreporting.eu); this is a legacy proposal, not a current limit.

ECCAIRS 2 is described by EASA as a web-based platform for the structured collection of occurrence data, and its project management has moved to EASA (aviationreporting.eu). ICAO materials presented in 2026 state that ICAO uses ECCAIRS 2 as its ADREP solution (www.icao.int) and that more than **1,000** safety systems already transmit reports automatically to it (www.icao.int).

Controlled identity boundary

The boundary between internal handling and outbound data can be written as a short checklist:

- **Inside the organisation:** reporter identity and free-text narratives stay with the designated persons, and wider dissemination uses disidentified information.
- **Outbound payload:** names and personal details are omitted when transferring reports to the authority, as the Commission guidance encourages.
- **Authority databases:** the Regulation requires that no personal details are ever recorded in the national database.
- **Pre-submission check:** a scrub of narrative fields before the message leaves the organisation, because the Commission's evaluation recorded occasional transfers of personal data through human error.
- **Mandatory fields:** relevant mandatory data fields cannot be left blank, and 'Unknown' is the permitted value when information is missing.

Portal, E5X upload and API: what receipts exist

EASA describes the machine-to-machine (API) and E5X upload options as available only to registered organisations (easa.europa.eu). In the European reporting portal, an E5X validation or upload generates an automatic confirmation email to the reporter (help.aviationreporting.eu), and the records in the file are saved as Original Reports (help.aviationreporting.eu). Unregistered reporters receive a reference number by email only if they supply an address (help.aviationreporting.eu). Each portal organisation account is tied to one authority: an organisation must use a different account for each competent authority (help.aviationreporting.eu), which matters for multi-state operators. Registered users only see reports sent since their account was created (aviationreporting.eu), and submitted data is transmitted onward to the ECR (help.aviationreporting.eu), a retention point for any platform that relies on the portal as its record.

No readable authority page promised a formal acknowledgement time, and the Regulation text reviewed contains no fixed deadline for acknowledging a reporter. The receipts documented are therefore channel behaviours (confirmation email, reference number) rather than legal acknowledgements, and the ledger should store whatever the channel returns.

National differences

Table 3 compares what ten authorities' pages literally say. It is a snapshot from pages opened in October 2026 and several pages are undated, so each should be re-checked with the authority before design.

Authority	Documented route for organisations	Integration or receipt detail stated
Germany (LBA)	ECCAIRS 2 portal is the only permitted route since 15 Feb 2023 (www.lba.de)	API for SMS passes (www.lba.de); manual upload of SMS-generated e5x files if no API (www.lba.de); account request must come from a member of management personnel (www.lba.de)
France (DSAC)	E5X or API upload script among the modes presented in a March 2026 webinar	Mandatory update of the upload script authentication (www.ecologie.gouv.fr); a report must be ticked for sharing with DSAC (www.ecologie.gouv.fr); accounts deactivate after 90 days without login (www.ecologie.gouv.fr)
Sweden (Transportstyrelsen)	ECCAIRS 2 portal, API or E5X upload; earlier E5X mailbox no longer used (www.transportstyrelsen.se)	API metadata names the receiving authority (www.transportstyrelsen.se); latest taxonomy retrievable via API (www.transportstyrelsen.se)
Malta (Transport Malta CAD)	National Centrik portal accepts an uploaded .e5x file (www.transport.gov.mt)	Submissions rejected unless mandatory fields are populated; the CAD uploads to ECCAIRS 2 and the ECR (www.transport.gov.mt)
Spain (AESAs)	Form, or .e5x/.e5f files by email as an alternative (www.seguridadaerea.gob.es)	72 hours from knowledge of the occurrence (www.seguridadaerea.gob.es)
Ireland (IAA)	ECCAIRS-compatible E5x files sent directly to the IAA (www.iaa.ie)	Option requires development work by the reporter (www.iaa.ie)
Poland (ULC)	ECCAIRS 2 account for organisations requested by online form (ulc.gov.pl)	Page dated March 2023; confirm current practice
Denmark (Trafikstyrelsen)	E2 administrator ("gatekeeper") appointed by the organisation (en.trafikstyrelsen.dk)	Gatekeeper is accountable to the organisation's Accountable Manager
Netherlands (ILT)	Report via the operator's SMS or EASA form (www.ilent.nl)	No receipt detail on the page
Austria (Austro Control)	2022 letter recommends registering to configure the E2 API (aeroclub.at)	Page may be superseded; confirm current practice

The comparison shows three patterns. Some authorities have closed older routes (Germany's portal is the only permitted channel; Sweden no longer uses its mailbox). Some keep file-based routes (Spain, Ireland, Malta). And account governance differs: Germany ties account requests to management personnel, Denmark to the Accountable Manager. For an AOC operating in several States, the contract needs a per-authority adapter, not one global "submit" button. The German 72-hour wording is likewise "not later than 72 hours after knowledge of the event" (www.lba.de), matching the Regulation, while Malta words it as 72 hours "of the event" (www.transport.gov.mt), which an adapter should surface to users rather than normalise away.

Implementation Considerations and Process Changes

Buy, integrate or build

Where a competent authority provides an ECCAIRS-compatible reporting system, EASA's FAQ says an organisation reporting through it need not have its own ECCAIRS-compatible system (easa.europa.eu). A small operator can therefore meet the format duty using the portal manually, and the ledger problem becomes one of recording what was done in the portal. Larger operators with an existing SMS face the integration question.

Vendor pages show that E5X or ECCAIRS output is a common SMS feature, always as vendor claims. One provider states that marking an occurrence for submission sends it automatically to the local authority following the E5X protocol (www.idealgen.com), and its taxonomy is said to be configured to the ECCAIRS equivalent (www.idealgen.com). Its help documentation notes that ECCAIRS export configuration is an admin-only feature (coruson.help.idealgen.com) and can export a single report to the authority (coruson.help.idealgen.com). Other vendors list ECCAIRS integrations (www.asms-pro.com) (www.trustflight.com), state that the SMS follows the ECCAIRS protocol (www.aviatize.com), or offer confidential or anonymous reporting options (skylegs.com). These statements are not independent benchmarks, and no public test of authority acceptance across vendors was found.

Table 4 frames the routes. It is a decision aid, not a ranking.

Route	What it is	Fits when	Limits to check
Authority portal, manual	Operator keys or uploads reports in the competent authority's ECCAIRS 2 portal	Low volume, no SMS integration need	Duplicate entry; ledger kept outside the portal; portal history only from account creation
Existing SMS with E5X or API export	Vendor SMS generates E5X or calls the authority API	A supported SMS already holds the intake	Mapping control, who owns awareness events, per-authority adapters
Authority API, direct	Operator system calls the authority's API after registration	High volume, one or two authorities	Sandbox and account process; taxonomy upkeep
Custom integration build (build-to-order software studios)	Software studio builds an intake and ledger layer around the operator's existing systems and data sources	Operator wants an evidence ledger and workflow across several tools	Not an off-the-shelf SMS or ECCAIRS platform; no authority acceptance, certification or ECCAIRS experience is implied here and must be verified in diligence

The table shows that the choice is less about "which ECCAIRS product" than about who owns the evidence events. A custom build suits an operator that needs the ledger across tools; it does not remove the operator's legal duties or its competent authority's requirements. Where an established SMS or reporting platform already meets the need, that category is the more direct answer.

Questions to ask any supplier or integrator

- **Awareness model:** Does the product record detection, reporter notification and organisation awareness as separate events with named humans?

- **Version chain:** Does every submission keep the exact payload and link to the prior version?
- **Receipts:** What does the target authority actually return, and is it stored unaltered?
- **Identity:** Can reporter identity be held under a restricted class and excluded from outbound payloads, consistent with Article 16?
- **Authority adapters:** Which authorities, channels and taxonomy versions are supported, and who maintains them?
- **Follow-up:** Can the system record a "no risk identified" decision and due dates keyed to reporter notification?
- **Retention:** Can records meet the operator's retention rule? EASA's AMC states a default minimum of **five years** where no other period is specified (www.easa.europa.eu), starting when a record is created or last amended.
- **Information security:** For operators, ORO.GEN.200A now brings an information security management system into the picture (eur-lex.europa.eu).

Process changes inside the operator

Four process changes usually accompany the ledger: define "awareness" in the operator's approved procedure and have the competent authority see it; keep the SMS feedback loop that the AMC expects of all reporting systems; retain reports the submitter judged reportable so decisions can be reconstructed; and protect records from alteration and theft as ORO.GEN.220 requires. The management system must be scaled to the operator's size and complexity, so a small operator's ledger can be simpler than a large airline's, provided the decision events remain traceable.

Go-live checks

Before connecting a production intake to an authority, a pragmatic test plan covers:

- **Sandbox run:** a test submission to the authority's test environment where one exists.
- **Mapping review:** a sample of internal events mapped to the current mandatory list and ECCAIRS fields, reviewed by the designated person.
- **Mandatory-field rejection:** confirmation that incomplete reports are caught before submission, since some portals reject them.
- **Receipt capture:** confirmation that the acknowledgement or reference number is stored.
- **Correction path:** a test of a second version that supersedes the first.
- **Data-quality sample:** a periodic check of initial against stored reports, consistent with Article 7(3).

Data Analysis and Evidence

Published figures give scale and data-quality context, not a benchmark for any one operator. Several come from different years and sources and should not be added together.

- **Central repository growth:** The Commission's 2020 report records growth from **1,125,264** reports at the end of 2014 to **2,548,578** in 2019 (eur-lex.europa.eu).

- **Recent volume:** EASA's Annual Safety Review 2025 says about **690,000** occurrence records were collected in the ECR over 2023 and 2024 and that the 2024 reporting rate was the highest since 2016 (www.easa.europa.eu).
- **National volumes:** Ireland's aviation authority reports **13,439** occurrence reports from Irish AOC holders in 2024 (www.iaa.ie). Sweden's authority states about 8,000 to 9,000 unique reports per year (www.transportstyrelsen.se). These are not comparable populations.
- **Regulation effect:** The Commission's evaluation estimated that the data-quality provisions made reports about 10% more complete (edz.bib.uni-mannheim.de).

Two cautions apply. First, no public benchmark was found for the elapsed time between organisation awareness and authority acknowledgement across operators, so the 31-hour figure in the worked example must not be read as typical. Second, the figures above come from different regulators with different counting rules, and the Irish and Swedish numbers measure different things. What the data support is a narrower claim: volumes are large, the Commission's evaluation estimated that the Regulation's data-quality provisions made reports approximately 10% more complete, and structured, validated fields at the point of intake support the completeness that an operator can influence.

Implications and Future Directions

Three developments should shape platform decisions over the next planning cycle. The first is list churn. Implementing Regulation 2026/1821 has already replaced the annexes, and a taxonomy or list change recurs unpredictably. A ledger that stores the list version and taxonomy version used for each reportability decision survives such changes better than a hard-coded mapping.

The second is channel consolidation. Authorities have moved toward ECCAIRS 2 accounts and APIs, and some have closed older routes. French operators using an upload script were told to update authentication, an example of integration maintenance that has to be budgeted. An adapter layer needs a named owner.

The third is the interplay with information security and just-culture governance. Operators now fall under Part-IS requirements through ORO.GEN.200A, and the Regulation's identity protections apply to the very system that stores the ledger. Any artificial intelligence tool that reads free-text narratives sees personal data, and a classification suggestion is not a reportability decision. The contract keeps the decision with a named human, which is consistent with Article 6(1)'s independent handling. No source retrieved for this report evaluated AI-assisted classification against authority acceptance, so any such use should be treated as unproven.

Frequently Asked Questions (FAQs)

Do all occurrences have to be reported within 72 hours?

No. The 72-hour limits attach to mandatory occurrences and to defined actors and triggers: individuals to their organisation and organisations to the authority, each with an exceptional-circumstances allowance for the individual duty. Voluntary reports are handled differently.

What does the follow-up requirement mean in practice?

Where analysis identifies an actual or potential risk, preliminary results and actions are due within 30 days of reporter notification, and final results in principle within three months.

How does this relate to ECCAIRS and E5X?

The Regulation requires ECCAIRS and ADREP compatible formats. E5X is one means of achieving that for organisations, and authorities specify the channel.

Can occurrence data be exchanged directly between operator and authority?

Yes, through the channels each authority documents, such as an API or E5X upload for registered organisations. Details are national, as Table 3 shows.

Is a seven-day acknowledgement to the reporter required?

None was found in the Regulation text reviewed for this report. Operators should check national procedures and their competent authority rather than assume one.

Conclusion

Regulation 376/2014 sets legal anchors for an occurrence-reporting design, but it does not define a single "awareness" timestamp, and guidance gives different start points for ordinary reports, automated detections and retrospective reports. The sound response is an evidence-event contract with separate events for detection, reporter notification, organisation awareness, reportability decision, classification, disidentification, submission, receipt, correction and follow-up, each carrying a UTC timestamp, a named human role and an access class.

The contract also manages revision risk. The mandatory list changed with effect from 17 August 2026, the EASA easy-access edition predates it, and national channels differ in route, account governance and receipts. Choosing between a portal, an SMS export or a custom integration is therefore a question of which party owns the evidence and the per-authority adapter. This report is analysis from public sources as of October 2026; operators should confirm requirements with their competent authority and keep their approved procedures as the controlling document.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://eur-lex.europa.eu/eli/reg/2014/376/oj/eng>
2. <https://easa.europa.eu/faq/98235>
3. <https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-occurrence-reporting?page=14>
4. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML?uri=CELEX:02012R0965-20260525>
5. <https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-occurrence-reporting?page=3>

6. <https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-occurrence-reporting?page=13>
7. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML?uri=CELEX:32014R0376>
8. https://www.lba.de/DE/Luftfahrtunternehmen/Ereignismeldungen/Functions_Kacheln/Kachel_4/Eccairs2_Node.html
9. <https://www.transportstyrelsen.se/sv/luftfart/olyckor-och-tillbud/luftfartshandelser/eccairs-2/teknisk-information>
10. <https://eur-lex.europa.eu/legal-content/EN/ALL?uri=CELEX:32026R1821>
11. <https://www.easa.europa.eu/en/regulations/occurrence-reporting>
12. <https://eur-lex.europa.eu/legal-content/EN/TXT?uri=CELEX:52020DC0733>
13. https://www.iaa.ie/docs/default-source/publications/corporate-publications/performance/iaa-annual-safety-performance-review-2024.pdf?sfvrsn=5115c0db_4
14. <https://eur-lex.europa.eu/legal-content/EN/ALL?uri=CELEX:32015R1018>
15. <https://www.easa.europa.eu/en/document-library/regulations/commission-implementing-regulation-eu-20261821>
16. <https://eur-lex.europa.eu/legal-content/EN/ALL?uri=CELEX:32020R2034>
17. <https://edz.bib.uni-mannheim.de/edz/pdf/swd/2021/swd-2021-0030-en.pdf>
18. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
19. <https://www.ideagen.com/regulations/eccairs>
20. <https://www.easa.europa.eu/en/node/120863?page=17>
21. https://www.transport.gov.mt/CAD-OR-Iss3_Rev0-Information-and-Guidance-on-Mandatory-and-Voluntary-Occurrence-Reporting.pdf-f11096
22. https://aviationreporting.eu/sites/default/files/2022-07/ECG%20Chapter%20_v1.0.pdf
23. <https://aviationreporting.eu/sites/default/files/2023-01/E5x%20implementation%20for%20Organisations.pdf>
24. <https://aviationreporting.eu/en/ElectronicReporting>
25. <https://aviationreporting.eu/en/taxonomy-browser>
26. <https://aviationreporting.eu/en/eccairs>
27. <https://www.icao.int/sites/default/files/APAC/Meetings/2026/2026%20ADREP%20and%20ECCAIR2/Presentations/Module%202%20E2%80%93%20Introduction%20to%20ECCAIRS%202.pdf>
28. <https://www.icao.int/sites/default/files/APAC/Meetings/2026/2026%20ICAO%20EASA%20Forum/Presentations/Agenda%205%20-%20E2%20in%20support%20of%20Annex%2013%20-%20Annex%2019%20SARPs.pdf>
29. <https://easa.europa.eu/en/domains/safety-management/aviation-safety-reporting/aviation-safety-reporting-organisations>
30. <https://help.aviationreporting.eu/books/reporting-portal/page/46-report-as-an-organisation>
31. <https://help.aviationreporting.eu/books/reporting-portal/page/3-report-without-registration>
32. <https://help.aviationreporting.eu/books/reporting-portal/page/43-registration-of-an-organisation>
33. <https://aviationreporting.eu/en/node/40>
34. <https://help.aviationreporting.eu/books/reporting-portal/page/1-introduction>
35. https://www.ecologie.gouv.fr/sites/default/files/documents/Webinaires_Notifier_mars_2026.pdf
36. <https://www.transportstyrelsen.se/sv/luftfart/olyckor-och-tillbud/luftfartshandelser/eccairs-2/inrapportering-i-eccairs-2>
37. <https://www.seguridadearea.gob.es/es/ambitos/gestion-de-la-seguridad-operacional/sistema-de-notificaci%C3%B3n-de-sucesos/notifica-un-suceso/notificaci%C3%B3n-de-profesionales-y-organizaciones>

- 38. <https://www.iaa.ie/safety/safety-reporting/reporting-options>
- 39. <https://ulc.gov.pl/en/safety-management/aviation-occurrences/reporting-of-aviation-occurrences>
- 40. <https://en.trafikstyrelsen.dk/civil-aviation/reporting/reporting-of-occurrence>
- 41. <https://www.ilent.nl/ilt-luchtvaartautoriteit/voorvallen-luchtvaart>
- 42. https://aeroclub.at/uploads/download/SIL_LFA_SAM_001.pdf
- 43. <https://www.lba.de/DE/Luftfahrtunternehmen/Ereignismeldungen/Allgemeines/Allgemeines.html>
- 44. <https://coruson.help.ideagen.com/hc/en-gb/articles/360013348239-Configuring-an-Export-Service-for-ECCAIRS>
- 45. <https://www.asms-pro.com/products.aspx>
- 46. <https://www.trustflight.com?p=3119>
- 47. <https://www.aviatize.com/features/safety-management>
- 48. <https://skylegs.com/safety-management-system>
- 49. https://www.easa.europa.eu/sites/default/files/dfu/annual_safety_review_2025.pdf
- 50. https://www.transportstyrelsen.se/globalassets/global/luftfart/seminarier_och_information/2024/afsr-var-2024/hantering-av-handelserapporter-inom-luftfart.pdf

THE PUBLISHER

About LANDING.AERO

LANDING.AERO builds custom software for aviation operations teams at airlines, charter operators and flight departments. It is based in Montreal.

What it builds

Operations tools that reduce manual steps in day-to-day flight operations; integration of existing systems and data sources into one operational picture; workflow automation; real-time operational dashboards; bridges between legacy systems and modern applications; and mobile apps for staff in the field. Each application is designed around the operator's own workflows rather than sold as an off-the-shelf platform.

How it works

Work starts with discovery of the operator's workflows, continues with iterative development alongside the operator's team, and includes integration with the tools already in use and ongoing support.

Its own tools

LANDING.AERO also publishes small tools for aviation professionals, including UTC Alarm, which sets alarms in Zulu time, and NOTAM Notifier, announced for NOTAM change alerts on chosen airports.

Visit

See LANDING.AERO and its projects.

Articles published here explain general practice and cite their primary sources, naming the jurisdiction of any rule they describe. They are not operational, regulatory or legal advice, do not replace an operator's approved procedures or manuals, and requirements change.

Website: <https://www.landing.aero>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.