Consultation response: Field 61, "Cause of the personal data breach"

Consultation: EDPB common template for personal data breach notification, version 1.0. Public consultation, feedback period 10 June to 5 August 2026.

Respondent: Alpha Data Consult (CVR 44987317), an independent consultancy specialising in personal data breach analysis and data protection, established in Denmark (www.alphadataconsult.dk); publisher of the GDPR data breach dashboard (www.gdprdatabrud.dk). Contact: Pradip Shrestha.

Date: 3 August 2026

Scope of this comment: Section 3.2 of the template, Field 61 ("Cause of the personal data breach"). Comments on Field 60 and Field 94 are submitted separately. This comment continues an argument opened in our Field 60 comment: several Field 60 incident types cannot be classified from the label alone, because their nature depends on the cause recorded here.

Summary position

We support the existence of Field 61 and the two distinctions built into its options: where the cause originated (internal or external) and whether it was deliberate. These are the right axes. The EDPB's own breach notification guidance organises its case material by risk source first and intent second, and the cause classifications used in European incident reporting are projections of the same two axes. Five defects in the drafting prevent the field from doing its analytical work. The two questions are fused into a single selection, so partial knowledge cannot be recorded. The axes are undefined at exactly the boundaries the EDPB's own case examples occupy. Breaches with no human actor have no option at all. "Malicious" prejudges motive, which the EDPB's own guidance treats as unknowable, and a single selection cannot record breaches that arrive as a chain of acts. Nothing binds Field 61 to Field 60, so the form accepts contradictory nature/cause pairs as clean data. Each defect has a remedy that uses structures the template already contains.

1. The issue

Field 61 offers six options: a) internal non malicious, b) internal malicious, c) external non malicious, d) external malicious, e) to be determined (available only for incomplete notifications), and f) unknown. The template marks fields that permit multiple selections (Field 40, "Allow multiple"); Field 61 carries no such marking, so we read it as a single selection.

1. **One selection fuses two questions.** Options (a) to (d) are the four combinations of two independent determinations: the origin of the cause, and the intent behind it. Origin is typically a matter of record early in an investigation; intent is an inference that often arrives later. A reporter who knows the origin but not yet the intent has no option that reflects what is known: recording "external, intent not yet determined" is impossible, and the escape values operate only on both questions at once. The field therefore forces exactly the guessing that corrupts comparability across authorities.

2. **The axes are undefined at the boundaries the EDPB's own cases occupy.** Is a former employee who copied data during employment internal or external? Is the staff of a processor (a party the template itself collects in Field 40) internal or external? The draft does not say, so different reporters will answer differently for the same facts.
3. **Breaches without a human actor have no option.** A flood, a fire, or a spontaneous technical failure has no actor and no intent; all four substantive options presume both. These breaches are not marginal: the availability breach type is defined by the EDPB as "accidental or unauthorised loss of access to, or destruction of" personal data, and the taxonomies in production at European level classify accidents, disasters, and failures as distinct incident classes.
4. **"Malicious" prejudges motive, and a single selection cannot record a chain.** Whether an act was deliberate can be established from evidence; whether it was malicious requires knowing why. The EDPB's own case material accepts that a controller may be left without any "reassurance on the intentions" of an actor even where the act was plainly deliberate. Deliberate but benign acts (data taken home to work on) and lawful intentional acts (a seizure) fit neither "malicious" nor "non malicious". Separately, breaches commonly arrive as chains (an external fraudster succeeding through an internal act), and a single fused selection forces the reporter to choose between the attacker's cause and the enabler's cause, a choice different reporters will make differently.
5. **Fields 60 and 61 are unlinked.** The form will accept Field 60 = "personal data sent by mistake" together with Field 61 = "internal malicious" and record the contradiction as valid data. Because nature and cause are one classification decision split across two fields, the split is safe only if the fields are validated together.

2. The proposal

Recommendation 1: decompose Field 61 into its two constituent questions. We recommend that Field 61 be decomposed into the two questions its present options combine. First, origin of the cause: internal; external; no human actor; to be determined; unknown. Second, asked only where a human acted, intent: intentional; unintentional; to be determined; unknown. The current four options are fully preserved as the four combinations of the two answers; nothing is discarded. Each question carries its own escape values, retaining the template's discipline: "to be determined" only while a notification is incomplete, "unknown" as a final, investigated answer. This decomposition is what allows a notification to be completed in phases without guessing: a first notification can record "external + to be determined" and the complete notification "external + intentional", with nothing guessed at either stage. Figure 1 shows the proposed structure.

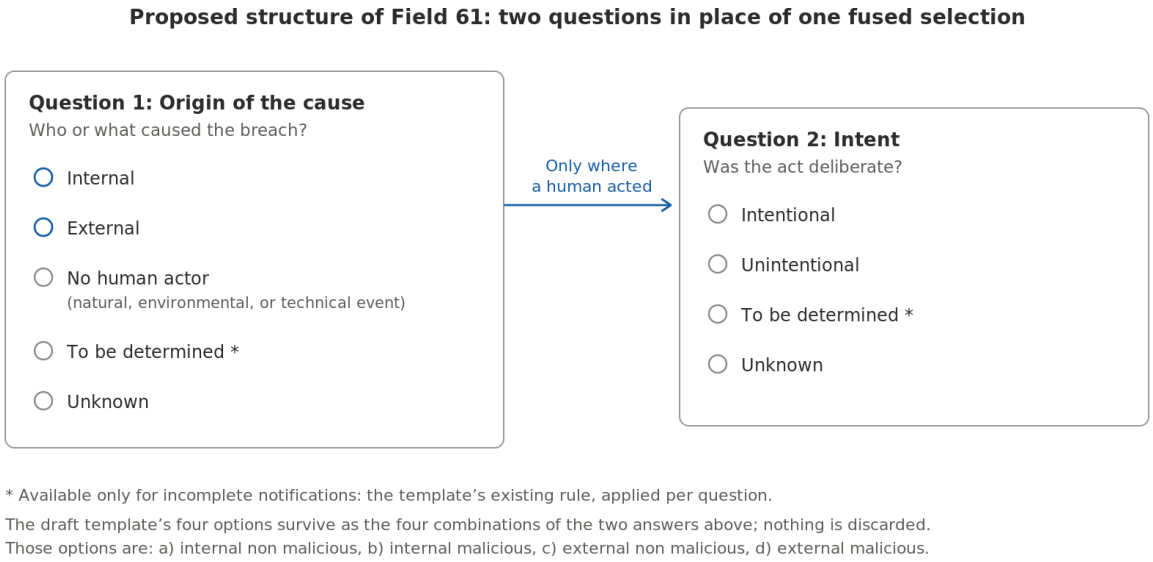

Figure 1. The proposed decomposition of Field 61 (Recommendations 1 and 2)

Recommendation 2: complete the origin question and define its boundaries. We recommend adding the class no human actor (natural, environmental, or technical event) for breaches in which no person acted and the intent question does not apply. We further recommend defining the two human classes at their boundaries: an actor is classified by status at the time of the initiating act, which resolves the former-employee case; the controller's processors fall on the internal side (the template already identifies them in Field 40); independent third parties fall on the external side.

Recommendation 3: define intent on the act, and classify chains by the initiating cause. We recommend renaming the intent axis intentional / unintentional, in line with the vocabulary of the EDPB's own guidance, and defining it on the act: an incident is intentional where the act that led to the breach was deliberate, irrespective of motive and of whether the scale of the outcome was intended. Where a breach is a chain of acts, we recommend that the classification record the initiating cause, with the chain described in Field 62, which already asks for the root cause and for the facts on which the reporter's decision is grounded.

Recommendation 4: complete Fields 60 and 61 together and validate them against each other. Our Field 60 comment recommends restructuring that field on the ENISA incident taxonomy in production at Datatilsynet, the Danish Data Protection Agency. We recommend that the two fields then validate each other mechanically: each origin/intent combination admits only a small set of Level-1 natures, and a notification recording an inadmissible pair can be flagged at the point of entry rather than becoming noise in European statistics.

Field 61 (origin + intent)	Admissible Field 60 Level-1 natures
Internal + intentional	Malicious activity/abuse; Physical and deliberate incidents
Internal + unintentional	Unintentional incidents; Errors and malfunctions
External + intentional	Malicious activity; Physical and deliberate; Interception; Legal
External + unintentional	Unintentional incidents; Interruptions
No human actor	Accidents; Errors and malfunctions; Interruptions
Either question unresolved	Unknown

3. Evidence from the EDPB's own guidance

EDPB Guidelines 01/2021 (Examples regarding personal data breach notification) supply every element of the proposal.

The two axes, in the EDPB's order. The Guidelines organise their case material by risk source (ransomware, data exfiltration attacks, internal human risk source, lost or stolen devices and paper, mispostal, social engineering) and resolve intent within the source: "Since these types of breaches can be both intentional and unintentional…" (para 71, under the heading "Internal human risk source"). CASE No. 08 (deliberate exfiltration by an employee) and CASE No. 09 ("accidental transmission… an unintentional human error") sit side by side in that one section: same origin, opposite intent, different classification and obligations. Origin first, intent second is the EDPB's own analytical sequence; the draft field fuses what the guidance keeps distinct.

Intent is decided on the act, not the motive or the outcome. In CASE No. 08 the controller "does not have any kind of reassurance on the intentions of the employee". The act (copying) is plainly deliberate; the motive is unknowable. In CASE No. 18, "the attacker was probably not aiming at collecting personal data" (para 129), yet the incident is unambiguously an intentional breach. An intent axis defined on the act is answerable from evidence; "malicious" is not.

Chains are the normal case, not the exception. The Guidelines require the controller to "investigate the method of infiltration" (para 27). CASE No. 17 is a chain: a "malicious party" deceives a contact-centre operator who follows the company's own validation procedure, which the EDPB then judges "clearly to be refined" (para 126). CASE No. 18 is a chain whose first link was never established: the company "was unable to detect how the attacker was able to gain access… but it supposed that an infected email was to blame". The template itself expects chains: Field 125 attaches both the ransomware note and the phishing message for a single incident.

Draft Field 61 defect	EDPB guidance that exposes it
Fused origin/intent selection	Guidelines Section 4 heading + para 71 (intent resolved within origin); CASE 08 vs CASE 09
Undefined internal/external boundary	CASE 08 (the "ex-employee"); template Field 40 (processors)
No option for non-human events	para 5 (availability breach: "accidental or unauthorised… destruction")
"Malicious" prejudges motive	para 74 (no "reassurance on the intentions"); para 5 ("unauthorised or accidental")
Intent judged on outcome	para 129 (attacker "probably not aiming at collecting personal data")
Single selection, chained causes	para 27 ("method of infiltration"); CASES 17, 18; Field 125

4. The proposal reflects existing supervisory practice

Datatilsynet classifies several thousand notified breaches a year on a taxonomy "largely based on ENISA's 2016 Threat Taxonomy" (our translation). Its ten Level-1 categories embed exactly the distinctions proposed here: deliberateness is built into the categories (physical and deliberate incidents; unintentional incidents; malicious activity), non-human classes exist and are used (accidents; errors and malfunctions; interruptions), and unknown is a production category, evidence that a reserved value for the undetermined does not degrade national statistics. Notably, the Danish taxonomy keeps "deliberate" (forsætlig) and "malicious" (ondsindet) as distinct concepts, which the draft field collapses; and Datatilsynet records that a single notification can concern several incident types, so production practice already accommodates incidents that span more than one category.

ENISA's own incident reporting practice points the same way. The root-cause categories used for over a decade in EU security incident reporting (system failures, human errors, malicious actions, natural phenomena, third-party failures) are projections of the two questions proposed here, including two classes (system failures, natural phenomena) that the draft Field 61 cannot express at all.

5. The remedy uses structures the template already contains

No new data collection is required. The evidence that answers both questions is already gathered by the form: Field 51 records how the breach was discovered, Field 62 asks for a description of the nature, the root cause "if possible", and "on what facts your decision is grounded", and Field 125 attaches the artefacts: the ransomware note, the phishing message, the misdirected communication. The escape-value discipline ("to be determined" only for incomplete notifications) already exists in the draft and is simply applied per question. Nor does the proposal strain the template's implementation model: the consultation describes the template as "primarily designed to be implemented by DPAs via an IT tool" which "incorporates rules to collect certain information only when necessary", and a conditional intent question and cross-field validation are native to exactly that design. The validation in Recommendation 4 is a rule set for an electronic form, not a new field. The cause classification produced here does further work the template already anticipates:

together with the circumstances that contributed to the breach, it is what selects the preventive measures recorded in Field 94, addressed in our separate comment on that field.

6. The GDPR notification within the proposed single-entry point

The proposed single-entry point will carry the Article 33 notification through the same channel as reports made under other Union instruments, and the EDPB and EDPS have observed that several of those instruments run on shorter deadlines than the GDPR's, recommending more harmonisation between the notification regimes (EDPB-EDPS Joint Opinion 2/2026, Section 8). The proposal therefore strengthens the GDPR notification process while remaining fully within the GDPR reporting framework. Article 33(4) already provides that information "may be provided in phases"; a Field 61 decomposed into origin and intent, with escape values per question, is what makes that phasing real for the cause of the breach. A controller can record at an early stage what is evidenced at an early stage, and complete the classification as the investigation matures, without ever revising an answer in front of the authorities reading the shared record. The GDPR template remains the authoritative account of the personal data breach; this proposal borrows no requirement from any other regime. It asks only that the GDPR's own cause field support what the GDPR's own notification design already provides for.

7. Recommendations, in brief

In summary, we recommend:

1. that Field 61 be decomposed into two questions, origin of the cause (internal / external / no human actor) and, for human origins, intent (intentional / unintentional), each with its own "to be determined" (incomplete notifications only) and "unknown" (final). The current four options survive as the four combinations.
2. that the origin boundaries be defined: actor status at the time of the initiating act; processors internal; independent third parties external.
3. that intent be defined on the act, not the motive or the outcome, and that chained breaches be classified by the initiating cause, with the chain described in Field 62.
4. that Fields 60 and 61 be completed together and validated against each other, per the admissibility table in section 2.

This gives the cause field the analytical capacity that our Field 60 comment and the template's own design (which reads nature, cause, and description as one record) already presuppose, and it does so with the options, evidence fields, and disciplines the draft template already contains.

References

- EDPB, Template for personal data breach notification, version 1.0, public consultation (feedback period 10 June to 5 August 2026): https://www.edpb.europa.eu/public-consultations/template-for-personal-data-breach-notification_en
- EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, version 2.0, adopted 14 December 2021: paras 5, 27, 71, 74, 126, 129; CASE Nos. 08, 09, 17, 18; Section 4 ("Internal human risk source"). https://www.edpb.europa.eu/documents/guideline/guidelines-012021-on-examples-regarding-personal-data-breach-notification_en
- Datatilsynet, "Hændelsestyper: Definitioner på typer af brud på persondatasikkerheden" (taxonomy basis, Level-1 categories, category definitions): https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/dokumentation-og-forklaringer/haendelsestyper-definitioner-paa-typer-af-brud-paa-persondatasikkerheden
- ENISA, Threat Taxonomy (2016), as cited by Datatilsynet: https://www.enisa.europa.eu/sites/default/files/all_files/Threat%20taxonomy%20v%202016.xlsx
- ENISA, Telecom Security Incidents 2024 (root-cause categories in EU incident reporting): https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA_Telecom_Security_Incidents_2024_en_1.pdf
- EDPB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted 10 February 2026, Section 8 (single-entry point; notification deadlines; harmonisation recommendation): https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en