Consultation response

Field 60, “Nature of the incident”

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 60 (“Nature of the incident”). Comments on Field 61 and Field 94 are submitted separately.

Summary position

We support the introduction of a common template. A common reporting instrument is a significant step towards more comparable and useful breach data. To realise that benefit, Field 60 requires a clearer classification structure. As drafted, it is a flat list of twenty-five incident types with no classification logic, and several items cannot be classified reliably from their labels alone. We recommend structuring Field 60 around the established European taxonomy already used by the Danish Data Protection Agency to classify personal data breaches.

1. The issue

Field 60 currently offers a single, flat list of twenty-five incident types (a to y). Three characteristics limit its usefulness:

1. **It has no hierarchy.** Vectors (phishing), techniques (ransomware), events (device lost), outcomes (unintended publication), and states (security vulnerability) sit at one level. A list that mixes levels cannot be aggregated or trended consistently, which is the core purpose of collecting this information.
2. **Some items bundle distinct incident natures.** A single selection is made to stand for events that belong to different categories.
3. **Some items cannot be classified from the label alone.** Their nature depends on the intent behind the incident and the surrounding circumstances, which the item does not capture.

The second and third characteristics are not cosmetic. Because a common template exists to make breach data comparable across all supervisory authorities in the EEA, an item that is classified inconsistently at the point of entry corrupts the resulting statistics at source. Field 60 is a mandatory field: every notification includes a selection from this list, so a defect in the list propagates into every record collected.

2. The proposal

Recommendation 1: adopt an established, hierarchical taxonomy. We recommend that Field 60 classify the nature of the incident using the ENISA Threat Taxonomy, structured hierarchically, with the template's current twenty-five items retained as sub-types beneath the top-level categories. Nothing is discarded; the existing list gains the parent structure and classification logic it lacks.

The taxonomy is already in production. Datatilsynet, the Danish Data Protection Agency, documents that its breach taxonomy "is largely based on ENISA's 2016 Threat Taxonomy" (our translation). It has categorised reported breaches since April 2020, aligned the taxonomy with the ENISA structure in January 2023, and now applies it to several thousand notifications a year. Its published statistics use the ten Level-1 categories, which are the top level of the ENISA taxonomy. The labels below are our translation. Datatilsynet publishes the taxonomy in Danish, and the original Danish labels are shown in parentheses:

1. Physical and deliberate incidents (Fysiske og forsætlige hændelser)
2. Unintentional incidents (Utilsigtede hændelser)
3. Accidents (Ulykker)
4. Errors and malfunctions (Fejl og funktionsfejl)
5. Interruptions (Afbrydelser)
6. Interception and eavesdropping (Aflytning/opsnapning)
7. Malicious activity and abuse (Ondsindet aktivitet/misbrug)
8. Legal (Juridisk)
9. Other (Andet)
10. Unknown (Ukendt)

Adopting this structure gives the template a taxonomy that is European in origin, proven in production at a supervisory authority, full-spectrum rather than attack-centred, and directly comparable with ENISA's own threat reporting. A hierarchical taxonomy improves comparability, trend analysis, and statistical reporting across supervisory authorities without increasing the reporting burden on organisations.

Recommendation 2: split the compound items. Where a single item bundles two distinct natures, we recommend separating it so that one selection denotes one nature. This applies to item (i) "device lost or stolen", item (o) "paper lost, stolen, or left insecure", and item (p) "personal data deleted/destroyed" (deletion and destruction).

Recommendation 3: classify incident nature using cause and supporting evidence. Where an item's nature depends on intent, we recommend completing Field 60 in conjunction with Field 61 (cause of the breach) and the descriptive and evidential fields the form already collects (Field 51, how the breach was discovered; Field 62, further description of the nature; Field 125, attachments), rather

than as a standalone selection. This applies to item (u) “unauthorised data modification”, item (w) “verbal unauthorised disclosure”, and the deletion branch of item (p).

3. Evidence

The following five items illustrate the two defects. They fall into two groups.

Conflation: the item bundles distinct natures.

- **(i) Device lost or stolen.** An accidental loss is an unintentional incident; a theft is a physical, deliberate act. These are different Level-1 categories, and the reporter is asked to record both under one label.
- **(o) Paper lost, stolen, or left insecure.** Paper lost or left insecure is unintentional; paper stolen is a physical, deliberate act.

Under-determination: the nature cannot be decided from the label.

- **(u) Unauthorised data modification.** This may be an accidental change or deliberate tampering.
- **(w) Verbal unauthorised disclosure.** This may be an inadvertent slip or a deliberate leak.
- **(p) Personal data deleted/destroyed** fails both ways: “deleted” versus “destroyed” is a conflation, and “deleted” alone spans three categories: an accidental deletion (unintentional), a software or hardware fault (errors and malfunctions), and a deliberate destruction (malicious activity).

The template’s own guidance already resolves these by intent and circumstance. The draft Field 60 asks reporters to commit to a nature that the EDPB’s own guidance says cannot be determined from the surface event. In EDPB Guidelines 01/2021 (Examples regarding personal data breach notification):

- Each breach type is defined as “unauthorised or accidental” (para 5): a confidentiality breach is “unauthorised or accidental disclosure”, an integrity breach is “unauthorised or accidental alteration”, and an availability breach is “accidental or unauthorised loss of access to, or destruction of” personal data. Disclosure, alteration, and destruction are each, by definition, either malicious or accidental.
- Human-source breaches “can be both intentional and unintentional” (para 71).
- Two paired cases demonstrate it: CASE No. 08 is a deliberate exfiltration by an employee who “maliciously copied the data”; CASE No. 09 is an “accidental transmission … an unintentional human error caused by inattentiveness”. The same broad scenario receives a different classification and different obligations depending on intent.

Field 60 item	Defect	EDPB guidance that resolves it
(i) device lost or stolen	conflation	Guidelines 01/2021, Section 5 para 85 (“the loss or theft of portable devices … circumstances”); para 5 (availability = “accidental or unauthorised loss”)
(o) paper lost, stolen, insecure	conflation	Guidelines 01/2021, CASE No. 12 (stolen paper); Section 5 para 85
(p) deleted/destroyed	conflation and under-determination	Guidelines 01/2021, para 5 (availability = “accidental or unauthorised … destruction”); CASES 01 to 04 (malicious destruction)
(u) unauthorised modification	under-determination	Guidelines 01/2021, para 5 (integrity = “unauthorised or accidental alteration”)
(w) verbal disclosure	under-determination	Guidelines 01/2021, para 5 (confidentiality = “unauthorised or accidental disclosure”); para 71; CASE 08 vs CASE 09

4. The remedy uses structures the template already contains

Recommendation 3 asks for no new data collection. The evidence needed to determine the nature of these incidents is already gathered by the form: Field 51 records how the breach was discovered, Field 62 invites a further description of the nature, and Field 125 attaches supporting material such as a ransomware note, a phishing message, or the communication sent to the wrong recipient. We recommend interpreting the nature classification in the light of the information already collected by the form and the cause recorded in Field 61, rather than making the decision from Field 60 in isolation.

5. Recommendations, in brief

We recommend:

1. Restructuring Field 60 as a hierarchical taxonomy based on the ENISA Threat Taxonomy, adopting its ten Level-1 categories as parents and re-parenting the current twenty-five items as sub-types.
2. Splitting the compound items that bundle distinct natures: separating loss from theft in (i) and (o), and deletion from destruction in (p).
3. Completing Field 60 together with Field 61 and the descriptive and evidential fields (51, 62, 125) for the items whose nature depends on intent, namely (u), (w), and the deletion branch of (p).

This aligns the template with an established European taxonomy, with the proven practice of the Danish Data Protection Agency, and with the EDPB’s own published guidance, and it does so without discarding the work already reflected in the current list.

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, 71, and Section 5 para 85; CASE Nos. 01 to 04, 08, 09, and 12. 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