Consultation response: Field 94, "Relevant measures taken to prevent similar 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 4.4 of the template, Field 94 ("Relevant measures taken to prevent similar personal data breach"). Comments on Field 60 and Field 61 are submitted separately. This comment completes an argument opened in those two: our Field 61 comment concludes that the cause classification, together with the circumstances that contributed to the breach, is what selects the preventive measures recorded here.

Summary position

We support the existence of Field 94 and the decision to collect preventive measures as a structured list rather than free text alone, since structured measures data is what makes prevention comparable across notifications and across authorities. The fifteen options are a fair union of the measure families that appear in the EDPB's own breach notification guidance. Four defects in the drafting prevent the field from doing its work. The field permits a single selection, although the same guidance recommends measures in combination and derives more than one measure from a single breach. The list is unordered, mixing organisational and technical measures, and it includes one option that remedies the breach that occurred rather than preventing a similar one. Nothing connects the recorded measures to the nature recorded in Field 60 or the cause recorded in Field 61, although the field's own label asks for relevant measures. No measure can be marked as taken or as proposed, although the section heading above the field provides for both. Each defect has a remedy that uses structures the template already contains.

1. The issue

Field 94 is mandatory and offers fifteen options: a) anonymisation, b) backup / recovery plan, c) change of processes, d) data encryption, e) data protection and information security policies, f) data protection and security training, g) erasure of the data, h) incident log, i) levels of access to data, j) logical access control (e.g. MFA), k) periodic audits, l) physical access control, m) pseudonymisation, n) up-to-date IT systems, and o) other measures, to be specified in Field 95.

1. **The field permits one selection where the answer is a combination.** The template marks fields that permit multiple selections (Field 40, "Allow multiple"); Field 94 carries no such marking, so we read it as a single selection. Preventive measures, however, arrive in sets. The Guidelines introduce their measure lists with "a combination of the below mentioned measures" (paras 83, 104), and the case material bears this out: in CASE No. 17 the EDPB derives both a refined validation process and out-of-band multi-factor authentication from one breach, which in this field's vocabulary is option c) and option j) at once. A reporter who has taken four measures and can record one will either select arbitrarily or route the remainder into free text, and the structured data loses precisely what the list exists to capture.

2. **The list is unordered, and it mixes prevention with remediation.** The options run together measures on the state of the data (anonymisation, pseudonymisation, encryption), access controls (levels of access, logical, physical), organisational measures (change of processes, policies, training, audits, incident log), and technical maintenance (backup and recovery, up-to-date IT systems), in no discernible order. One option belongs to a different question altogether: g) erasure of the data addresses the consequences of the breach that occurred, which is the subject of Field 92 ("Measures taken to address the personal data breach and to mitigate its consequences"), and prevents nothing about a similar breach. A related slip is already visible in the draft: the tooltip of Field 95 states that a description is expected "if you answered with 'Other measures' in the previous question m)", although other measures is option o). The list appears to have been re-lettered without the cross-reference following.
3. **Nothing binds the measures to the cause or the nature of the breach.** The field asks for relevant measures, but relevance is not a property a list can assert about itself: a measure is relevant to the cause and nature of the breach, or it is not. Training answers a human-error cause; encryption answers a lost-device nature; neither answers the other. As drafted, the form accepts Field 61 = "internal non malicious" (a human error) together with Field 94 = "physical access control" alone, and records the pair as clean data, although the recorded measure does not engage the recorded cause. Our Field 60 and Field 61 comments each arrive at this point: nature and cause constrain what is admissible elsewhere in the record. Field 94 is where that constraint has its effect, and the draft leaves the three fields unconnected.
4. **A measure cannot be marked as taken or as proposed.** The section heading above the field reads "Measures taken (or proposed to be taken) to prevent similar personal data breach"; the field label drops the parenthesis and asks only for measures taken. In a notification made in phases, that distinction carries most of the information: at a first notification a controller has typically proposed measures and completed few of them. With no status per measure, the reporter either records proposals as taken or omits them, and a follow-up notification cannot record what has since been completed.

2. The proposal

Recommendation 1: permit multiple selections. We recommend that Field 94 be marked "Allow multiple", using the device the template already applies to Field 40. This is the smallest of the changes proposed here and the one on which the others depend, since a measures field that holds one value cannot describe the combinations the Guidelines themselves recommend.

Recommendation 2: order the list by measure family, and confine it to prevention. We recommend grouping the options under the two families named in the Guidelines' own section titles, organisational measures (change of processes; data protection and information security policies; data protection and security training; periodic audits; incident log; levels of access to data) and technical measures (anonymisation; pseudonymisation; data encryption; logical access control; physical access control; backup / recovery plan; up-to-date IT systems). We further recommend moving erasure of the data out of this list, since it is a remedial measure whose subject is Field 92. Grouping costs nothing in an electronic form and makes a fifteen-item list legible; re-lettering also provides the occasion to correct the cross-reference in the Field 95 tooltip.

Recommendation 3: record a status for each selected measure. We recommend that each selected measure carry a status, taken or proposed, aligning the field with the section heading above it. This is the discipline our Field 61 comment proposes for the cause axes, applied here: a first notification records proposed measures as proposed, and the complete notification records which of them have been taken, so that progress between notification

phases becomes structured data rather than prose. Article 33(4) already provides that information may be given in phases, and a status per measure is what makes that provision operable for this field.

Recommendation 4: read Field 94 together with Fields 60 and 61. The cause and the nature recorded earlier in the form make some measures expected and others unexpected. We do not propose strict validation here, as the relation between causes and measures is many-to-many, and the Guidelines are explicit that the controller decides "which measures fit the given situation the most". We recommend instead a coherence prompt at the point of entry: where the recorded cause is a human error and no organisational measure is selected, or the recorded nature is a lost or stolen device and encryption is not among the measures, the form invites the reporter to confirm the selection or to explain it in Field 95. The prompt costs a reporter with a considered answer a single confirmation, and it catches the incoherent record at source rather than in analysis. The table below is indicative rather than exhaustive.

Field 61 (origin + intent)	Measures the recorded cause makes expected
Internal + unintentional	training; change of processes; policies; levels of access to data
Internal + intentional	levels of access to data; logical access control; incident log; periodic audits
External + intentional	logical access control; up-to-date IT systems; backup / recovery plan; training
External + unintentional	change of processes; policies
No human actor	backup / recovery plan; up-to-date IT systems; physical access control

The nature recorded in Field 60 sharpens the expectation further: a lost-device breach expects encryption, which is the first advisable measure in the Guidelines' own list for that risk source, and a mispostal breach expects a changed sending process and training.

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 guidance organises preventive measures by risk source. Each risk-source section of the Guidelines closes with a section titled "Organizational and technical measures for preventing / mitigating the impacts" of that source: ransomware (section 2.5), data exfiltration attacks (3.4), internal human risk source (4.3), lost or stolen devices and paper documents (5.4), and mispostal (6.5). The measures differ in each. Section 4.3 opens with training, awareness programmes, and access-control policy; section 5.4 opens with device encryption; section 6.5 with sending practices and message delay. The EDPB's own structure states the third defect's remedy as a table of contents: which preventive measures are advisable is a function of the source of the breach. The draft field flattens those five source-specific lists into one list read without reference to the source.

Measures come in combinations, fitted to the case. The Guidelines introduce their measure lists with "a combination of the below mentioned measures", applied "depending on the unique features of the case" (paras 83, 104), and preface every list with the caution that

it is "by no means exclusive or comprehensive", the controller deciding "which measures fit the given situation the most". Both halves are instructive: plurality is assumed, which is Recommendation 1, and fit to the situation is the test of relevance, which is Recommendation 4.

The EDPB derives the measure from the cause. CASE No. 17 is the worked example. A fraudster passes a contact centre's client validation using publicly available information, and billing data is sent to an illegitimate address. The EDPB reasons from cause to measure: "The prior client validation process is clearly to be refined in light of this case" (para 126); static knowledge-based authentication "is not recommended" (para 127); and "the introduction of an out-of-band multi-factor authentication method would solve the problem" (para 128). The cause is social engineering of a weak process, and the measures are a change of processes and logical access control, two options, both selected by the cause. The draft field records neither the plurality nor the derivation.

Draft Field 94 defect	EDPB guidance that exposes it
Single selection	paras 83, 104 ("a combination of the below mentioned measures"); CASE 17 (two measures from one cause)
Unordered list, families not distinguished	the Guidelines' own section titles: "Organizational and technical measures", per risk source (sections 2.5, 3.4, 4.3, 5.4, 6.5)
Measures unlinked to cause and nature	the same five sections (measures organised by risk source); para 126 (measure derived from cause)
Relevance unassessable	paras 49, 84, 105 (the controller decides "which measures fit the given situation the most")

4. The remedy uses structures the template already contains

No new data collection is required. The multi-selection marker exists and is used elsewhere in the template (Field 40, "Allow multiple"). The status proposed in Recommendation 3 restores a distinction the template's own section heading already draws. The inputs the coherence prompt needs are already collected: Field 60 records the nature, Field 61 the cause, and Field 62 the root cause and "on what facts your decision is grounded". Field 95 already provides the free-text companion in which a prompted reporter explains an unexpected selection, and its tooltip already invites exactly that: "do not hesitate to describe further measures taken after the breach, or to be taken, if you think it is relevant". 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 grouped multi-selection list with a status per item and a conditional prompt is native to that design. The machinery is present; what the draft does not yet do is connect it, although the form already holds the cause and the nature by the time the reporter reaches Field 94.

5. The measures record 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 recommended more harmonisation between the notification regimes (EDPB-EDPS Joint

Opinion 2/2026, Section 8). The recommendations above strengthen the GDPR measures record while remaining entirely within the GDPR framework, and they borrow no requirement from any other regime. The Joint Opinion also observes that the proposed changes to the notification threshold leave the controller's Article 32 obligations untouched. Those obligations are the reason Field 94 exists, and they do not vary with how many breaches reach a notification form. A measures record that holds combinations, distinguishes what has been taken from what is proposed, and can be read against the cause and the nature is what allows the notification to evidence Article 32 compliance in the way the template already sets out to do.

6. Recommendations, in brief

In summary, we recommend:

1. that Field 94 be marked "Allow multiple", the device the template already applies to Field 40.
2. that the options be grouped into organisational and technical measures, following the Guidelines' own section titles, that "erasure of the data" be moved to the subject of Field 92, and that the cross-reference in the Field 95 tooltip be corrected.
3. that each selected measure carry a status, taken or proposed, aligning the field with the section heading above it and making progress between notification phases visible.
4. that Field 94 be read together with Fields 60 and 61 through a coherence prompt at the point of entry, per the indicative table in section 2, so that an unexpected pairing of cause and measure is confirmed or explained in Field 95 rather than recorded without comment.

This gives the measures field the capacity that the template's own section heading, its free-text companion, and the Guidelines' own treatment of preventive measures already presuppose, and it does so with the markers, 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 49, 83, 84, 104, 105, 126 to 128; CASE No. 17; sections 2.5, 3.4, 4.3, 5.4, 6.5 ("Organizational and technical measures for preventing / mitigating the impacts"). 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, 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; harmonisation recommendation; Article 32 obligations unaffected): https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en