Siemens Healthineers AG | Regulatory Affairs | August 5, 2026

Consultation response · Medical technology

Commentary on the EDPB Template for personal data breach notification (Article 33 GDPR)

Subject: EDPB Template for personal data breach notification, Version 1.0, adopted on 8 June 2026, released on 10 June 2026, currently under public consultation
Perspective: manufacturers of medical devices and in vitro diagnostics operating across borders
Consultation period: 10 June to 5 August 2026, 23:59 CEST

I. Key points

> The initiative deserves support. The fragmentation of national notification forms creates effort without any gain in protection, particularly for organisations operating across borders, and a harmonised instrument is the logical consequence of the one-stop-shop principle. The present draft does not, however, meet the objective it sets for itself. According to its own rationale it is meant to save time and cost, especially for smaller organisations without a dedicated data protection officer, yet even in the most trivial notifiable case it calls for 41 mandatory entries, nine of them free-text justifications. By comparison, the German Länder forms examined manage with a little over two dozen fields and roughly 18 mandatory entries.

The proposals below require no redesign. They pursue three points:

- Separating the question *whether* to notify from the question *what* to notify.
  The risk test is the normative preliminary question under Article 33(1) GDPR. The template places it at field 89, in the middle of the form, and thereby suggests an expectation to notify that the Regulation does not impose. This is the most important point of this commentary.
- Grading the notification burden by risk.
  The template offers a single path. A misdirected email without sensitive data costs virtually the same as a breach involving health data.
- Guidance rather than surface area.
  Where the template deploys conditional logic, it works well. Where it refrains from doing so, notably for special categories of data, it shifts the entire risk of misclassification onto the user.

II. Benchmark: the template measured against its own objective

The EDPB has justified the template by the aim of enabling controllers and supervisory authorities to structure, harmonise and unify their notification processes, of facilitating timely notification and of supporting the authorities' assessment. This is expressly intended to save time and cost, in particular for smaller organisations without their own data protection officer or legal department. The initiative forms part of the Helsinki Statement, whose objective is to facilitate GDPR compliance and to strengthen consistency across Europe.

A legal consideration is added to this. Article 33(3) GDPR defines the content of a notification as a minimum content ("at least"). Whatever the template asks for beyond that

minimum is therefore not ultra vires. It does, however, require justification, measured against its necessity for the authority's assessment and against the simplification objective the EDPB itself has formulated. The following comments operate at that level, not at the level of competence.

They are aligned to that benchmark and to no benchmark imported from outside. Every one of them is designed to achieve the stated objective more effectively, not to slow the initiative down.

III. Findings: what the template costs in an individual case

The template comprises 126 numbered fields across seven sections. 26 of these are section headings, leaving 100 question fields. The conditional logic works and suppresses a considerable proportion of them. It does not, however, differentiate by severity. Counted against the logic set out in the draft, three typical constellations produce the following:

Constellation (in each case a complete, timely initial notification)	visible fields	mandatory fields	of which mandatory free text
Misdirected email without special categories of data, sent to an external recipient	55	42	9
Internal misdirection to the wrong recipients, attachment containing remuneration data	54	41	9
Misdirection involving health data, high risk, communication to data subjects, two Member States affected	64	50	10

Two observations carry this commentary:

First, proportionality is absent throughout.
A single mandatory field separates the trivial misdirection from the case involving remuneration data; the health data case with a cross-border element lies nine above it. In terms of effort, the form does not distinguish between an incident at the notification threshold and a serious breach.

Second, it is the mandatory free-text entries, not the selection fields, that drive the burden.
In all three constellations, fields 51, 62, 63, 66, 71, 76, 90, 92 and 95 are mandatory narrative justifications. Field 63 calls for a description of the systems, software, services and infrastructure affected, including their locations, at a level of granularity prescribed in the tooltip, and it does so even for the plain misdirection of an email. Within 72 hours, alongside root cause analysis and containment, that is disproportionate for high-volume, low-risk cases.

The figures given are lower bounds. The contact data fields marked with an asterisk are, according to the template's own footnote, presented in simplified form and will be collected "in a structured way" in the actual form, that is to say broken down into several individual fields; field 117 requires an entry for each Member State affected.

Comparison with existing notification forms

For calibration, the official notification forms of two German Länder were counted. The Baden-Württemberg form comprises 24 fields, of which roughly 18 are mandatory; the Berlin form comprises 23 fields. The two are structurally near-identical and evidently derived from a common model, which suggests that a large proportion of the Länder work at that order

of magnitude. The comparison is only sound if one disclosure is made: the Länder forms achieve their low field count by bundling matters into free-text fields. A single field headed "description of the data breach" there captures, all at once, the location, the parties involved, the manner of detection, the internal escalation and any third-party knowledge, that is to say everything the template distributes across a dozen individual fields. Part of the template's higher field count is therefore not additional burden but atomisation, which serves machine processing and is to that extent welcome.

The difference in burden lies elsewhere and remains. The Länder forms call for roughly 18 largely narrative mandatory entries, which the notifying party may frame in its own words. The template calls for 41 to 50 mandatory entries, nine of them structured mandatory free-text entries, on top of dozens of atomised selection fields, including the infrastructure description with location details even in a trivial case. It is not the number of fields as such but the level of detail demanded per entry, measured against the 72-hour deadline, that is the yardstick against which the draft falls short of its promise of simplification.

The international picture is no more uniform. Some regimes make do with a concise statutory catalogue, for instance Brazil with twelve mandatory entries (Article 6 § 2 Resolução CD/ANPD 15/2024) or Switzerland with seven categories of information (Article 15 DPO); others, such as Japan or New Zealand, require a similar number of individual entries to the present draft once the actual official notification form is examined, namely around 35 and 36 respectively, each counted at the official source. The international finding therefore confirms above all the methodological core of this commentary: field counts are no reliable yardstick unless the counting method and the degree of bundling are stated. What matters is the level of detail per entry measured against the notification deadline.

IV. Detailed commentary

Structure of each point: A. Summary, B. Provision concerned, C. Assessment, D. Suggested wording. The first marker indicates urgency, the second the effect of the proposal on the complexity of the form.

1. Separating the decision to notify from the content of the notification: a preliminary check placed up front

[core concern] [reduces complexity]

A. Summary

Article 33(1) GDPR ties the duty to notify to the risk test: notification is required unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The risk test is thus the normative preliminary question, and its outcome determines whether notification occurs at all. The template places it at field 89, in the middle of the form, after some eighty preceding fields. At the same time, nowhere does the form make visible that it can also serve the internal documentation duty under Article 33(5) GDPR.

B. Provision concerned

Field 89 in relation to the overall structure; Section 1 (type of notification). Evidence of the conflation: field 89(c) provides for *unlikely to result in a risk* as an element of the notification, and field 97(d) likewise for the constellation without high risk; fields 56(c) and 57(a) capture breaches without exfiltration and with encryption intact. The word *documentation* does not appear anywhere in the question catalogue. The benchmark otherwise is Guidelines 9/2022, which emphasise the primacy of the risk test over the decision to notify.

C. Assessment

Whoever opens the form has, in practical terms, already taken the decision to notify. From that point the form no longer asks whether notification is required, only what must be reported. The consequence is a structural bias towards precautionary notification: incidents that do not reach the threshold are notified as a precaution, because the form offers no other use. That burdens supervisory authorities, whose staffing situation is consistently described as strained in their annual reports, with matters that yield no gain in protection, and it burdens controllers with effort the Regulation does not impose on them. Both run counter to the stated objective. The proposal costs the EDPB little and reduces complexity substantially, because it keeps the majority of incidents out of the question catalogue altogether. It also elevates the template: from a mere notification form to an instrument that reflects both duties under Article 33 GDPR, notification under paragraph 1 and documentation under paragraph 5.

D. Suggested wording

> A preliminary block 0, "Preliminary check", placed before Section 1: *"(1) Is there a personal data breach within the meaning of Article 4(12) GDPR? (2) Does the assessment show that the breach is likely to result in a risk to the rights and freedoms of natural persons? Only if both questions are answered in the affirmative is the notification to be transmitted to the supervisory authority. If the second question is answered in the negative, the completed form serves as documentation under Article 33(5) GDPR and is not transmitted."*
>
> In addition, a marker in Section 1 identifying the purpose of use ("notification under Article 33(1)" / "documentation under Article 33(5)"), which in documentation mode reduces the set of mandatory fields to the information required by Article 33(5) GDPR.

2. Grading the notification burden by risk

[core concern] [reduces complexity]

A. Summary

The template knows a single path. Frequent low-risk incidents that only just cross the notification threshold pass through the same question catalogue as serious breaches. A simplified path for defined standard cases would serve the purpose of the template better than a uniform full catalogue.

B. Provision concerned

The overall structure, in particular the mandatory free-text fields 62, 63, 76 and 90. Further, Article 33(4) GDPR, which permits phased notification, and its implementation in fields 3 and 4.

C. Assessment

For typical high-volume cases, the misdirected email, incorrectly configured access rights, lost documents, the catalogue is out of proportion to what the authority stands to learn. The effect is counterproductive twice over: the controller cannot reach the level of detail demanded within 72 hours and files an incomplete notification followed by an update, while the authority processes the same matter more than once. The template does implement Article 33(4) GDPR cleanly; it recognises incomplete notifications and expressly reserves the option *To be determined* for them. What it does not say is which information it

already expects in the initial notification. That uncertainty generates follow-up notifications which clear labelling would render unnecessary. That it can be done differently is shown, incidentally, by the narratively bundled Länder forms: they leave it to the notifying party to determine the depth in which the facts can be presented within the deadline.

D. Suggested wording

> (a) Introduction of a simplified notification path for defined standard constellations with a reduced set of mandatory fields, in particular dispensing with the duty to describe the infrastructure (field 63) and to describe the methodology of the risk assessment (field 90), where no high risk arises and no special categories of data are affected.
>
> (b) A marker in the template identifying which fields are expected in the initial notification and which are reserved for the subsequent notification under Article 33(4) GDPR; clarification that the initial notification is not incomplete merely because deferred information is absent.

3. Special categories of data: linking them to the risk classification

[core concern] [complexity-neutral]

A. Summary

Field 70 captures biometric data (c), genetic data (j), health data (k) and employment-related health data (m) as distinct categories. Between that selection and the severity classification in field 87, as well as the risk outcome in field 89, there is no conditional logic whatsoever. A user can tick health data and nonetheless set severity to *minor* and risk to "unlikely to result in a risk", without the form displaying so much as a prompt.

B. Provision concerned

The linkage of field 70 with fields 87 and 89. The benchmark is Guidelines 9/2022, according to which special categories under Article 9 GDPR typically raise the level in the risk test.

C. Assessment

For medical technology this point is central. A breach affecting imaging data, findings, laboratory results or diagnostic outputs will in practice almost always yield a risk or a high risk in the risk test. The question is not whether notification occurs, but how quickly and with what content. A template that does not reflect that relationship shifts the risk of misclassification entirely onto the user, and specifically onto the user without a dedicated data protection officer, whom the template is meant, according to its own rationale, to assist. The proposal adds no field. It uses the conditional logic the template deploys throughout in any event, and replaces the need for advice with guidance. It does not narrow the assessment: a lower classification remains available, it merely has to be justified. That justification is required in field 90 in any event.

D. Suggested wording

> Conditional logic: where one of options (c), (j), (k) or (m) is ticked in field 70, field 89 defaults to *likely to result in a* risk and the following prompt is displayed: *"Special categories of personal data within the meaning of Article 9 GDPR are affected. A classification as 'unlikely to result in a risk' must be expressly justified in field 90 (see Guidelines 9/2022)."* Field 87 to default to *moderate* accordingly, with the option of justifying a lower classification.

4. Field 60: insufficient delineation, no priority rule, missing device categories

[needs revision] [complexity-neutral]

A. Summary

Field 60 offers 25 options for the type of incident. Several cover the same factual situation without the delineation being apparent, and there is no priority rule for cases in which more than one applies. At the same time, categories for incidents involving connected devices are missing.

B. Provision concerned

Field 60 and the associated list of options.

C. Assessment

The common case of incorrectly configured access rights can be assigned to at least options (a), (f), (g), (n) and (q); the display of data to the wrong recipient additionally to (h). The misdirection of an email falls simultaneously under (l), (r) and, where the distribution list is open, (s). Without a priority rule, different controllers will select different categories for the same facts. The taxonomy thereby fails its purpose: it is meant to make notifications comparable and to support the authorities' analysis, and it cannot do so if it is populated inconsistently. This is not an objection to the existence of the taxonomy. Controlled vocabularies are the precondition of any machine-readable exchange and are therefore expressly to be welcomed. The objection is directed solely at their delineation. From a medical technology perspective there is a further gap: incidents involving connected medical devices, for instance misconfigured device interfaces or unintended data outflows through remote service access, can only be captured incompletely under (m) *Misconfiguration* or (n) *Incorrect access permissions.* Precisely in the sector in which special categories of data are regularly affected, the taxonomy remains imprecise.

D. Suggested wording

> (a) Revision of the list to remove overlaps; where overlaps are unavoidable in substance, multiple selection with identification of a primary category and a priority rule set out in the tooltip.
>
> (b) Addition of device-related categories, for instance "misconfiguration of a connected device or device interface" and "data outflow via remote or service access".

5. Section 3.1: the date of detection is missing

[addition required] [replaces free text]

A. Summary

The heading of Section 3.1 reads *Date and time of the personal data breach and of its detection.* What is captured, however, is only the occurrence of the breach (fields 46, 47) and the point at which the controller became aware of it (field 48). There is no field for the point in time at which the breach was detected within the organisation.

B. Provision concerned

Section 3.1. Field 50 captures only the manner of detection, not its timing; field 52 captures a date only where awareness was conveyed from outside.

C. Assessment

The period under Article 33(1) GDPR begins when the controller becomes aware. In organisations with distributed responsibilities, a period regularly elapses between detection at the operational level and awareness at the level of the controller, and that period determines whether the deadline is met. If there is no structured field for it, the information migrates into the free text of field 53, whose tooltip mentions it by way of example. That serves neither side well: the controller cannot cleanly evidence compliance with the deadline, and the authority cannot analyse the information. In the multi-tier health sector, where manufacturers frequently act as processors for hospitals, this is the single most significant point in time in practice. The proposal increases the field count by one, but transfers content out of a mandatory free-text field into a structured field and therefore does not increase complexity on balance. It is, moreover, in the interest of the notifying party.

D. Suggested wording

> Addition in Section 3.1, alongside field 48: *"Date and time of detection of the breach within the organisation, where this preceded the controller becoming aware of it."* The tooltip to field 53 to be shortened accordingly.

6. Field 110: orientation on parallel notification duties

[addition required] [no new field]

A. Summary

Field 110 asks whether the incident has been notified to other supervisory or control bodies under other legislation. The question is framed retrospectively and names only the national cybersecurity authority by way of example. What is missing is orientation as to which regimes may come into play at all. That is precisely where most errors arise in practice.

B. Provision concerned

The tooltip to field 110. No additional field is proposed, expressly so.

C. Assessment

In a regulated environment, a data breach rarely triggers Article 33 GDPR alone. For manufacturers of medical devices, vigilance reporting under Article 87 MDR or Article 82 IVDR may apply, as may cybersecurity reporting under NIS2 and national implementing law, reporting to health data access bodies under the EHDS Regulation where health data are put to secondary use, the provisions of §§ 284 et seq. of the German Social Code Book V for social data, and, subject to Regulation (EU) 2026/1744 which has meanwhile entered into force, the reporting of serious incidents under Article 73 of the AI Act. None of these acts coordinates its reporting track with the others. A note in the tooltip costs no field, imposes nothing on controllers outside regulated sectors and forestalls the most common error, which is overlooking a second track. The delineation must be observed strictly, and for the same reason that this commentary counsels restraint elsewhere: the note must not create any notification content. It is pure orientation, not a question, not a duty and not part of the notification under Article 33 GDPR. In that form it does not go beyond the minimum content of Article 33(3) GDPR, nor does it touch upon the competence of the data protection supervisory authorities.

D. Suggested wording

> Extension of the tooltip to field 110: *"Note: in addition to the data protection notification duty, further independent reporting duties may exist, for instance under*

medical devices law, cybersecurity law, the law governing the secondary use of health data, the law governing artificial intelligence or social data protection law. Those reports are addressed to other bodies, follow their own deadlines and are not replaced by the notification under Article 33 GDPR. This note serves orientation only; it creates no data protection duty, and information on this subject does not form part of the notification under Article 33 GDPR."

7. Field 49: capturing reasons for delay in structured form

[desirable] [complexity-neutral]

A. Summary

Field 49 captures the reasons for a delayed notification under the second sentence of Article 33(1) GDPR as a pure free-text field. The visibility condition is implemented precisely and deserves support; the mode of capture falls short of the standard set by the remaining fields.

B. Provision concerned

Field 49.

C. Assessment

At precisely this point, where the information is legally sensitive and time pressure is at its greatest, a structured selection assists both sides: it relieves the controller of having to draft under pressure and renders the information analysable for the authority. A free-text supplement remains necessary alongside it.

D. Suggested wording

> A selection list placed ahead of field 49 setting out typified reasons (for instance: extent of the breach ascertainable only after investigation; awareness gained only through notification by a processor or third party; ongoing containment measures taking priority; coordination with authorities or law enforcement; failure of the organisation's own systems), together with a free-text field.

8. Machine readability, interfaces, modular extensibility

[strategic] [reduces complexity]

A. Summary

The template's footnote records that the fields presented in simplified form will be collected in structured form in the actual form. The technical implementation is therefore still open, and the EDPB has announced that it will decide on the timeline for practical implementation only after the consultation has closed. This is the right moment to specify it in an interface-capable manner.

B. Provision concerned

The overall structure and the implementation phase; the footnote to the fields marked with an asterisk.

C. Assessment

Anyone who demands more than 40 mandatory entries in an individual case must enable those entries to be populated from the systems in which the information is held in any event. That requires stable field identifiers, controlled vocabularies, a machine-readable

representation of the conditional logic and an interface for transmission. The benefit grows with the number of notifications and the number of authorities involved, and is therefore substantial precisely for the cross-border case the template addresses. The notification channels themselves remain a matter of national implementation; they currently range from an integrated online form, through a download with a separately requested upload link, to a portal with two-factor authentication. The EDPB cannot prescribe them. A machine-readable specification of the template is, however, the precondition for national implementations to converge rather than for the existing fragmentation to be built on top of a uniform form. Without it, the objective of unification is achieved on paper only. That the decision on the implementation timeline is still outstanding does not make the proposal secondary but urgent: it can be taken into the planning now without disruption, whereas after the timeline has been settled it can only be taken up against it. Extensibility points in the same direction: the sectoral differentiation of European data law, for instance in the EHDS context, will generate sector-specific additional information. An opening clause spares later fundamental revisions.

D. Suggested wording

> (a) Publication of a machine-readable field specification together with the template: stable field identifiers, controlled vocabularies for the selection fields, formal representation of the conditional logic.
>
> (b) A recommendation to the supervisory authorities to provide a uniform interface for transmission, permitting machine population from controllers' systems.
>
> (c) A note in the template documentation: *"The template may be extended by sector-specific supplementary modules. Such modules leave the basic structure and the notification content under Article 33 GDPR unaffected."*

9. Technical quality assurance before implementation

[editorial] [complexity-neutral]

A. Summary

A review of the consultation version has revealed inconsistencies in the conditional and option logic. For a draft they are unremarkable; since, however, the template proceeds directly into technical implementation by every supervisory authority, they should be resolved beforehand.

B. Provision concerned

Individual fields, in overview:

Field	Finding
83	The consequence question for availability breaches carries the visibility condition *visible only if Integrity = 1*. In a pure availability breach it therefore does not appear, whereas in an integrity breach it appears in addition to field 81. Apparently carried over from field 81, with substantive effect.
89	The options *unlikely to result in a risk* and *additional information is needed* both bear the letter (c). In the very field on which the notification threshold turns, the labelling ought to be unambiguous.

Field	Finding
100, 101	The visibility condition (*No they will not be informed*) does not distinguish between field 97(d) and field 97(e). The field content fits (e) alone; on the broader reading, controllers facing no high risk would be prompted to provide a justification under Article 34(3) GDPR, which does not apply there.
44	The logic column refers to an option (f); the selection list ends at (e).
53	The mandatory condition *Yes, if 41a* refers to a field that does not exist.
6, 3/4	Inconsistent labels: field 6 refers to *complementary/amended notification/withdraw*, fields 3 and 4 to *Follow-Up* and *Withdraw*. Consistent terminology is required for machine-readable implementation.
19, 33, 41	Incomplete indications as to mandatory status or visibility, diverging from the respective neighbouring fields.
118, 123	Field 123 is headed *EAA* instead of *EEA*; in field 118 several authorities are merged into a single line. The authority lists are flat and offer no assistance in allocation, which complicates selection precisely in the one-stop-shop section.

C. Assessment and D. Proposal

These points reflect the draft stage and are not intended here as criticism of the initiative. What is proposed is a technical review of the field logic before the binding version, combined with the machine-readable specification proposed under no. 8, which would render inconsistencies of this kind verifiable in future. Since the EDPB will decide on the timeline for practical implementation only after the consultation, a window is open for this which will have closed once implementation is released to the supervisory authorities.

V. Background: the multi-layer reporting regime in medical technology

The following overview explains the proposal made under no. 6. It does not form part of the commentary on the template; its purpose is to illustrate the scale of the coordination problem a single data breach involving health data can trigger.

Regime	Addressee	Deadline	Trigger and status
Article 33 GDPR	Lead supervisory authority (Article 56 GDPR)	72 hours from awareness	Risk to rights and freedoms. Practically always met where health data are involved. Directly applicable.
Article 34 GDPR	Data subjects	without undue delay	Where the risk is high. In the hospital context regularly through the institution as controller.
Article 87 MDR / Article 82 IVDR	Competent authority via EUDAMED	2 / 10 / 15 days	Serious incident. For manufacturers the principal second track. Directly applicable.

Regime	Addressee	Deadline	Trigger and status
Article 73 AI Act	Market surveillance authority	immediately	Serious incident involving high-risk AI. The AI Omnibus was published as Regulation (EU) 2026/1744 of 8 July 2026 in the Official Journal of 24 July 2026 and entered into force on 27 July 2026. The deferral of the high-risk obligations is therefore positive law: 2 December 2027 for stand-alone systems under Annex III, 2 August 2028 for systems embedded in products under Annex I, which is the typical medical device constellation. Article 73 itself has not been amended; the deferral operates through the applicability of the high-risk obligations to which the reporting duty attaches.
NIS2 and national implementing law	National cybersecurity authority	24-hour early warning, 72-hour notification	Cybersecurity incident at essential entities. Applicability to be assessed case by case.
EHDS Regulation	Health data access body	as provided under EHDS law	Breach in the context of secondary use. Implementation periods running.
§§ 284 et seq. SGB V	Competent body	as provided under social data law	Social data, in so far as processed for sickness funds or healthcare providers.

The deadlines do not run in parallel and cannot be synchronised; the data protection deadline is consistently the tightest. A single form cannot bring these tracks together, and it should not attempt to: the data protection notification is person-related, the medical device notification clinical and technical. It follows that the template requires no amendment beyond the note in field 110. It also follows, however, that coordinating the reporting tracks remains an open task for the European legislature which no standard form resolves. The AI Omnibus has changed nothing in that respect: it defers application dates, it does not coordinate reporting tracks.

VI. Concluding remarks

With a uniform template the EDPB pursues a sound and overdue approach. The proposals made here require no redesign but a better use of what the template can already do. Its conditional logic is carefully constructed in many places; it is simply not deployed where it would achieve the most, namely at the preliminary question of the duty to notify, at the grading by risk and at the special categories of data.

The first point remains the most important. So long as the form does not visibly separate the question whether notification is required from the question what must be reported, it will generate notifications the Regulation does not require and absorb effort that benefits neither the data subjects nor the supervisory authorities. An instrument which, according to its own rationale, is meant to assist smaller organisations without a dedicated data protection officer must first of all tell them when they need not complete it.

> Monitoring reservation. The data track of the Digital Omnibus (COM(2025) 837), comprising amendments to the GDPR, the ePrivacy Directive and the reporting duties under cybersecurity law, has not been concluded in Parliament; no position of the Parliament or of the Council is on record, and the EDPB and the EDPS have

issued a joint opinion. For the present response this has no consequences: Articles 33 and 34 GDPR apply unchanged, and every proposal made here attaches to those provisions alone. Should the data track come to affect the notification content under Article 33(3) GDPR, Section II (benchmark) and proposals 1 and 2 will require fresh examination. Until then no adjustment is called for.