Privacy4Cars
https://privacy4cars.com
privacyrights@privacy4cars.com

30 July 2026

European Data Protection Board
Via webform at
https://www.edpb.europa.eu/public-consultations/template-for-personal-data-breach-notification_en#no-back

Re: Comments Regarding the Personal Data Breach Template

Dear European Data Protection Board,

The Personal Data Breach Template draft Section 3 fields "Incident scenario" and "Cause" are built around discrete triggering events (an attack, an error, a misconfiguration, a lost device). They do not provide a way to record breaches whose root cause is the **sustained absence of a technical or organisational measure** to address a known, recurring, foreseeable exposure pathway, as opposed to a one-off human or system failure.

This gap matters because breaches of this kind are structurally different: they indicate non-compliance with Articles 5, 24, 25 and 32 GDPR rather than an isolated incident, and they are likely under-captured in notification data as a result.

Illustrative context

A concrete and large-scale example that 12 data protection authorities from Belgium, Bulgaria, Croatia, Estonia, Finland, Latvia, Lithuania, Poland, Romania, Slovenia, Spain, and the UK[1] have recently flagged as a massive-scale data breach: personal data stored in connected-vehicle systems (contacts, call/navigation history, paired-device and garage credentials, location history) that is not erased by Controllers such as leasing companies, rental providers, fleet operators, insurers, lenders, or car dealerships. When the data remains accessible to the next user without authorisation, this meets the Article 4(12) definition of a personal data breach (unauthorised access/disclosure), yet the underlying cause is not an attack or an isolated mistake: those 12 DPAs agreed that the root cause is the Controller's failure to implement objective, repeatable, auditable processes for deletion before transfer of custody, contrary to Articles 5(1)(f), 25 and 32 GDPR and consistent with the EDPB's own Guidelines 01/2020 on connected vehicles. Because this exposure recurs with every vehicle transaction rather than arising from a single incident, we believe it is likely significantly under-reported relative to its actual scale across the EU.

At Privacy4Cars we estimate about 4 in 5 vehicle transactions leave behind and cause to expose unencrypted personal data of Data Subjects in Europe. That is tens of million of non-reported data breach incidents per year related to change of ownership where the Controller is a dealership, a lender, or an insurer, and tens of millions more related to rental and shared corporate fleets where the Controller is a rental or car sharing company or a business with a vehicle fleet.

Specific proposed amendments

1. Section 3 – "Incident scenario" (currently ~25 predefined categories) Add a distinct category for: *"Personal data not erased/deprovisioned from a device or physical asset prior to transfer of custody, possession, or*

[1] Privacy4Cars, "GDPR Compliance: Your Obligation to Delete Personal Data from Vehicles: What 12 European Data Protection Regulators Say," accessed July 29, 2026, https://privacy4cars.biz/gdpr-compliance/.

ownership" — distinguished from "incorrect disposal of devices," which implies an active but mishandled disposal step, not an absent deletion process altogether.

2. Section 3 – "Cause" (currently classified along internal/external and malicious/non-malicious axes) Add a third dimension, or a qualifying sub-field, distinguishing:

- *Discrete event* (an identifiable single incident: attack, error, loss), from
- *Structural/systemic absence of a technical or organisational measure* addressing a known, recurring risk.

This allows DPAs to distinguish notifications reflecting a one-time lapse from those reflecting the absence of any compliance process, information relevant to enforcement prioritisation and to identifying sector-wide patterns. This information is important because DPAs determine the severity of GDPR fines by taking into account 10 determining criteria[2], one of which is precautionary measures (the amount of technical, organisational, and auditable preparation the Controller has previously implemented in compliance with GDPR).

3. Section 3 – "Pre-existing measures" / Section 4 – "Mitigation and prevention measures" Add an explicit binary/qualitative field: *"Did any objective and repeatable technical or organisational measure exist, prior to the breach, intended to prevent this category of incident?"* A "none existed" or "subjective processes" or "policy exists but processes are not repeatable" answers are materially different information from "a measure existed but was circumvented or failed," and the current free-text framing does not reliably surface that distinction.

Legal basis

- Art. 4(12) GDPR – definition of personal data breach includes unauthorised access/disclosure, regardless of whether it results from an attack or a process failure.
- Art. 5(1)(f) and Art. 32 GDPR – integrity, confidentiality, and appropriate technical/organisational security measures.
- Art. 5(1)(e) GDPR – storage limitation, requiring deletion once the original processing purpose ends (e.g., at end of a vehicle's use period by a given data subject).
- Art. 25 GDPR – data protection by design and by default, including at points of transfer of custody of data-bearing assets.
- Art. 5(2) and Art. 24 GDPR – accountability; deletion/erasure processes must be objective, repeatable, and demonstrable, not dependent on individual employee judgment.
- EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.

Requested action

We ask the EDPB to revise Section 3 of the template (incident scenario and cause taxonomies) and the related pre-existing/mitigation measures fields as described above, so that breach notifications can distinguish incidents caused by an absent or non-existent security process from incidents caused by a discrete attack or error. Without this distinction, the template's data will systematically under-represent, and DPAs will be less able to detect, breach patterns arising from Controllers' failure to implement Article 25/32 measures across recurring, foreseeable data flows such as the transfer of data-bearing physical assets.

Sincerely,

Privacy4Cars Privacy Team
privacyrights@privacy4cars.com

[2] Ben Wolford, "What are the GDPR Fines?," GDPR.eu, last modified February 13, 2019, https://gdpr.eu/fines/.