Submission to the EDPB's Public Consultation on the

Personal data breach template

Prighter Group

Vienna 05.08.2026

About Prighter and This Feedback

Prighter is a group of companies acting as the representative for over 2,000 companies under EU and non-EU data protection, digital governance and AI regulations, and providing software to simplify the compliance obligations stemming from these frameworks.

Prighter regularly needs to report data breaches on behalf of clients without an establishment in the EU and welcomes therefore the opportunity to give feedback on the template for data breach reporting used by authorities.

This feedback is mainly driven by the practical insights and challenges from the current data breach reporting processes and the vision of using some automation to operationalise the reporting process and make it more efficient.

Executive Summary

1. General Remarks

In its Guidelines 09/2022 as adopted 28 March 2023 the European Data Protection Board (EDPB) has concluded that companies without an establishment in the EU need to notify a data breach to every supervisory authority for which affected data subjects reside in their Member State. In the week of the submission to this public consultation Prighter needed to report a data breach on behalf of a client to all data protection authorities including all German ones, with the exemption of Luxembourg and Ireland. Prighter's process is to first collect all the data needed for the notifications from the client ("fact finding mission") to draft a master notification which serves as the source for then filling the different and individual forms. Filling one form and submitting the notification to one authority takes on average two hours for a trained legal team member. The obligation to report to all authorities therefor takes longer than the whole 72 hours deadline and can only be met with additional automation.

The three main reasons for the inefficiency are:

- the different online forms currently used by data protection authorities;
- the different processes of accessing the online forms and signing them; and
- the lack of automation in the individual process.

2. Feedback on the Template for the Data Breach Notification

2.1. General: Common Unique Field IDs

The template for the data breach form is intended to be implemented by data protection authorities across Member States. These Member State authorities use different languages in their proceedings.

Common unique field IDs allow for an easy understanding of the required input across all languages and even more important for a structured filling of the form with the opportunity to automate the process. The numbering of the "Field" column already used throughout this template (fields 1-125) are a simple version of such common unique identifier. Important is that the EDPB mandates that Member States carry such field IDs over unchanged into their national online forms and APIs.

2.2. On Section 2.1: About the data controller

Parts of the data breach form depend on whether the controller is established in the EU and therefore has a lead supervisory authority or not.

We recommend including a field at the beginning of the form in section 2.1. for the controller to select between established in the EU or not established in the EU. This would only make explicit what the template already assumes: rows 113 and 120 are each conditioned on this very status ("only if DC is based in EEA" and "only if DC is NOT based in EEA" respectively), yet the template never actually asks the controller to declare it.

Depending on the selection different field along the data breach form are visible such as:

- Representative (row 18 and 19)
- Section 6.2 and 6.3

2.3. On Row 25: National identification number

In some of the current online forms Member State authorities allow only a national ID issued in their specific country blocking reporting from any person without such ID. Because non-EU companies can rely on their representative in one Member State for communication with all authorities and do not need to appoint representatives in every Member State, such requirements of a National ID contradict the concept of the representative.

We recommend always allowing an identification of the reporting individual via an eIDAS authentication. We note that field 25 is already marked in the template as an optional field, to be implemented only where required; our recommendation therefore concerns the implementation guidance given to Member States, namely that wherever a national identification number is requested nationally, an eIDAS-based identification of the reporting individual must always be accepted as a sufficient alternative.

2.4. On Row 68 and 73: Number of Data Subjects and data records

Both rows indicate only one number to be specified by the controller for the affected data subjects and the concerned data records. In a cross-border breach involving also countries outside of the EU there is the difference between:

- the global overall number
- the number within the EU; and
- the number in the country for which the authority is competent.

Giving the overall global number in the data breach form has a significant impact on the risk assessment (e.g. worldwide 10 million data subjects are affected from which 100 000 are in Europe and only 10 are in Austria).

We recommend splitting the number in row 68 (and, for the same reason, in row 73) into at least the overall global number and the number related to the specific Member State. In cross-border cases a further breakdown per individual EEA country is already possible via the existing fields for the number of data subjects in the EEA per country (rows 116-118 and 121-123).

2.5. On Section 6

The template currently is structured in:

6.1.: Authorities other than data protection ones

6.2.: Data protection authorities for companies with an establishment

6.3.: Data protection authorities for companies without an establishment

We recommend changing the order to

6.1.: Data protection authorities for companies with an establishment (depending on the selection in 2.1.)

6.2: Data protection authorities for companies without an establishment (depending on the selection in 2.1.)

6.3.: Authorities other than data protection ones

To us it seems more intuitive to first ask for the data protection authorities before moving on to other authorities.

2.6. On Section 6.2 and 6.3 (current version)

Section 6.2. and 6.3. ask for various inputs on a list of Member States. In order to avoid duplication we recommend having one table with multiple columns for:

- lead supervisory authority (depending on the selection in 2.1.)
- List of EEA countries where the controller has an establishment (depending on the selection in 2.1.)
- Approximate number of data subjects per country
- List of EEA supervisory authority to which the breach has been or will be notified (depending on the selection in 2.1.)

Row 121 and 122 could be combined into one input asking for the number of data subject per country as a number.

3. Feedback on the Process of filing Data Breach Notifications in an online form

3.1. Authentication and Signature process

Some of the current online forms require an authentication to access the form and a signature process. In some cases the access is possible through an eIDAS authentication, but the signature is only allowed with signatures from a local trust service provider. This results in the effort of filling the form and being blocked in the end from filing it.

We recommend only an authentication process in the beginning, because this is sufficient to identify the person filing the notification. The signature process in the end does not give additional security. If data protection authorities still require the signature process at the end, it should allow for the same method as the authentication in the beginning.

Furthermore, some authorities require an eIDAS signature from the controller. However, eIDAS is an EU concept and non-EU controller are not able to obtain an eIDAS signature, because they have no access to a local trust service provider. We highly recommend removing such requirements, because it prevents non-EU companies from any communication with data protection authorities and therefore from reporting a data breach.

3.2. Explanation and Preview

Before filling an online form, a controller or representative should be clear about the procedural requirements and the required information. The ability to check the procedural requirements and preview authorities' online forms before starting to complete it, prevents frustrated efforts.

3.3. API Option

Even with one common data breach notification form the filling of 42 EU and additional EEA notification forms takes a significant amount of time. This would become much more efficient with an option to file the notifications form via an API.

The benefits of an API option are:

- Consistency of the notification and an increased quality;
- Cost reduction for controllers and therefore less reluctance to report;
- Adaptability for future changes especially the single entry point and the common notification template across other authorities as well;
- Secure communication