THE DATA LAWYERS

TO European Data Protection Board
FROM The Data Lawyers and Responders.NOW
DATE 5 AUGUST 2026

JOINT SUBMISSION BY THE DATA LAWYERS AND RESPONDERS.NOW ON THE EDPB DRAFT HARMONISED PERSONAL DATA BREACH NOTIFICATION FORM

1 INTRODUCTION

The Data Lawyers and Responders.NOW welcome the initiative of the European Data Protection Board to harmonise the personal data breach notification form across the European Economic Area. A single, standardised form reduces the administrative burden for controllers operating in multiple EU member states and promotes consistent supervisory practice.

While we note the other attachment categories listed in Field 125 raise similar questions, this submission focuses on one specific element: the fact that Field 125 invites controllers to attach a dated copy of the ransomware-note to their data breach notification. We respectfully submit that this field should be removed from the notification form or, at a minimum, remain strictly optional.

2 REMOVE OPTION TO SHARE DATED COPY OF THE RANSOMWARE-NOTE

Field 125 of the draft form invites controllers to attach up to ten categories of documents to their breach notification listed as follows:

- *Dated copy of the communication to the data subject*
- *Dated copy of the risk-assessment*
- *Dated copy of the research report into the data breach (cyberincidents)*
- *Dated copy of the ransomware-note*
- *Dated copy of the phishing-message*
- *Dated copy of the internal procedure to notify a data breach*
- *Dated copy of the internal policy to delete/destroy (outdated) personal data*
- *Dated copy of the communication to the wrong recipients*
- *Dated copy of the external notification/message of the data breach*
- *Other.*

We strongly recommend to – at least – remove the "*dated copy of the ransomware-note*" from this list because of the reasons listed below.

2.1 Disproportionate and ineffective

2.1.1 The notification obligation is limited to narrative information

Article 33(3) GDPR exhaustively defines the minimum content of a breach notification. It requires the controller to: (a) describe the nature of the breach, (b) communicate the contact details of the DPO, (c) describe the likely consequences, and (d) describe the measures taken or proposed. Article 33(3) GDPR does not require the production of documents as part of the notification itself.

2.1.2 Request is not appropriate, necessary and proportionate

Requesting copies of ransomware-notes, forensic research reports, internal policies, or risk assessments constitutes an exercise of investigative powers under Article 58(1)(a) GDPR, which empowers supervisory authorities to "order the controller and the processor [...] to provide any information it requires for the performance of its tasks". This power is subject to strict proportionality safeguards: Recital 129 GDPR requires that "each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case". The exercise of Article 58 GDPR powers must be assessed on a case-by-case basis, not embedded as a standing expectation in a harmonised template.

2.1.3 Practical concerns: forensic integrity

From an incident response perspective, Responders.NOW emphasises that premature disclosure of ransomware-notes and forensic findings can compromise ongoing negotiations with threat actors and jeopardise the integrity of forensic investigations. Attaching such materials to a notification form that may be processed by multiple handlers within an authority increases the risk of inadvertent disclosure and operational interference.

The ransomware-note often contains sensitive operational information, including specific instructions, deadlines, contact details, payment methods and, in some cases, unique identification codes. If controllers submit such material as part of the (initial) data breach notification, the risk of unnecessary dissemination of operationally sensitive information increases. In particular, it may adversely affect the course of ongoing negotiations, potentially leading the threat actor to terminate the negotiations, increase the ransom demand, accelerate the publication of exfiltrated data, or employ additional coercive measures, such as distributed denial-of-service (DDoS) attacks or directly contacting the victim's customers or employees.

3 ADDITIONAL REMARKS

In addition to the above, we emphasize the following:

- Requesting the list of documents should remain strictly optional, also taking into account the reasoning set out above. In addition, requesting all this information would slow down the process of informing the supervisory authority/-ies within 72 hours.
- It should be made clear that not providing the listed documents does not mean the supervisory authority/-ies concludes that such documentation is not in place.

The Data Lawyers and Responders.NOW remain available for further dialogue with the European Data Protection Board on how the harmonised notification form can be designed in a manner that respects the structural distinction between the notification obligation under Article 33 GDPR and the investigative powers under Article 58 GDPR, while ensuring that breach response remains effective and timely for all stakeholders involved.