

Template [2026] for personal data breach notification

Version 1.0

Adopted on 08 June 2026

Orange Restricted

Version history

Version	Date	Adoption information
version 1.0	08 June 2026	adoption of the template for public consultation

Table of Contents

1. Information on the personal data breach notification 1

1.1 Type of notification 1

2. Identification of the data controller and the reporting person 2

2.1 About the data controller 2

2.2 Identity of the reporting person 3

2.3 Name and contact details of the data protection officer or other contact point where more information can be obtained 4

2.4 Involvement of other parties 5

3. Initial information on the personal data breach 5

3.1 Date and time of the personal data breach and of its detection 5

3.2 Nature, circumstances and summary of the personal data breach 7

3.3 Categories and number of data subjects concerned 10

3.4 Categories and number of personal data records concerned 11

3.5 Measures in place when the personal data breach occurred 12

4. Further information on the personal data breach 13

4.1 Likely consequences of the personal data breach and potential adverse effects on data subjects 13

4.2 Assessment of the risk to the rights and freedoms of natural persons 15

4.3 Measures taken (or proposed to be taken) to address the personal data breach and to mitigate its possible adverse effects 15

4.4 Measures taken (or proposed to be taken) to prevent similar personal data breach 15

5. Communication to the data subjects 17

6. Possible other issues 19

6.1 Whether other authorities or bodies have been notified 19

6.2 Whether the personal data breach involves a cross-border processing 19

6.3 Whether the personal data breach involves a processing at non-EU establishments 23

7. Attachments 26

The European Data Protection Board has adopted the following template:

0	Field	Value	Tooltip	Mandatory	Business Logic
1	**1. Information on the personal data breach notification**				
2	1.1 Type of notification				
3	**Type of notification**	a) New Notification b) Follow-Up Notification	Indicate here if you notifying a new data breach or if you are amending a previous notification	Yes	
4	**Sub-type of notification**	a) Complete b) Incomplete c) Withdraw	Indicate here if you provide a complete notification, amend a preliminary (incomplete) notification or provide preliminary (incomplete) information to be amended. Complete (all required information can be provided) Incomplete (not all information can be provided right now) Withdraw (Cancel a previous Notification; e.g. duplicate, no risk after initial assessment)	Yes	Withdraw visible only if "Type of notification" = "follow-up notification"
5	**Reasons for withdrawing a previous notification**			Yes, if visible	visible only if "Type of notification" = "follow-up notification" and "Sub-type of follow-up notification" = "Withdraw"
6	**ID of previously notified personal data breach**		Please provide the ID of the previous personal data breach your are completing or amending.	Yes, if applicable	visible only if "Type of notification" =

Z komentarzem [A1]: Could you provide more potential grounds for withdrawal? These will need to be specified in the next step.
For example, where the event did not constitute a personal data breach — e.g. the discovery of documents intact, or the emergence of new circumstances.
As controllers, we need the form to clarify the following: What is the effect of withdrawing a notification? Will the supervisory authority continue to have access to both the initial/incomplete notification and the information on its withdrawal? Will withdrawal of the notification be mandatory in such cases? Will the authority be able to exercise its powers under Article 58 GDPR if it concludes that the withdrawal was not justified? As controllers, we need more information about the withdrawal of a notification in order to assess whether including such an option in the notification is justified

Z komentarzem [A2]: We understand that this is a number assigned according to the controller's own register, meaning it will not be a number assigned by the supervisory authorities, as indicated in paragraph 7 below.
If this field is to be mandatory, the authorities must ensure that controllers are informed of the reference numbers assigned to preliminary notifications, or provide an easy means of contact in such cases. At the same time, it appears that in the case of supplementary notifications submitted very soon after the preliminary notification (e.g. notifications made by telecommunications entities), the authority itself will not always manage to assign a reference number to the preliminary notification in time. For this reason, we suggest that this field be optional.

					"complementary/amended notification/withdraw". Check existence of a previously notified data breach
7	**Data controller's internal reference number**		Provide your internal reference number if any	No	
8	**2. Identification of the data controller and the reporting person**				
9	2.1 About the data controller				
10	**Type of Identifier**	a) CompanyID b) Organisation number c) VAT Number (…) […]		Yes, if applicable	optional field
11	**Identifier**			Yes, if applicable	optional field, Ask for selected identifier
12	**Name of the organisation**			Yes	
13	**Contact details***			Yes	
14	**Sector**	a) Private b) Public		No	
15	**Type of organisation**	a) Freelance or Microenterprise b) Small or Medium Enterprise c) Large Enterprise d) Others	If you consider your organisation not fitting in those four categories, please select “Others” and specify how.	No	only if private
16	**Further description of organisation type**			No	only if others
17	**Classification of economic activity**	A Agriculture, Forestry and Fishing B Mining and Quarrying C Manufacturing		No	

Z komentarzem [A3]: Throughout the document, it is necessary to maintain consistency in the use of defined terms.

Z komentarzem [A4]: This would need clarification at national level

Z komentarzem [A5]: Who to ask?

Z komentarzem [A6]: What are the distribution criteria? Or rather an organizational form?
If this information is necessary for the authorities to assess infringements, we suggest that the criteria for determining the type of organization be grounded in the regulations. That said, this solution may impose a significant burden on administrators, given the need to analyze this additional criterion.

		D Electricity, Gas, Steam and Air Conditioning Supply E Water Supply; Sewerage, Waste Management and Remediation Activities F Construction G Wholesale and Retail Trade H Transportation and Storage I Accommodation and Food Service Activities J Publishing, Broadcasting, and Content Production and Distribution Activities K Telecommunication, Computer Programming, Consulting, Computing Infrastructure and other Information Service Activities L Financial and Insurance Activities M Real Estate Activities N Professional, Scientific and Technical Activities O Administrative and Support Service Activities P Public Administration and Defence; Compulsory Social Security Q Education R Human Health and Social Work Activities S Arts, Sports and Recreation T Other Service Activities U Activities of Households as Employers and Undifferentiated Goods and Service-Producing Activities of Households for Own Use V Activities of Extraterritorial Organisations and Bodies			
18	**Name of representative in EEA**			Yes, if visible	only if controller not established in EEA
19	**Contact details* of representative in EEA**				
20	2.2 Identity of the reporting person				
21	**Name of the reporting person**			Yes	
22	**Contact details**			Yes	
23	**Function of the reporting person**	a) DPO b) Legal representative		Yes	

		c) Authorised representative or other (please specify)			
24	**Description of the function of the reporting person**			Yes, if visible	only if 23 is c) other
25	**National identification number**			Yes, if applicable	Optional field, implement only if required
26	**Accuracy & Responsibility**	Checkbox: Information on the liability for the accuracy of the information provided (can be combined with Art. 13 information)		Yes, if applicable	Optional field, implement only if required
27	2.3 Name and contact details of the data protection officer or other contact point where more information can be obtained				
28	**2.3.1 About the data protection officer**				
29	**Is a data protection officer designated?**			Yes	only if DPO not provided as reporting person in 1, yet
30	**Name of the DPO**			Yes	only if DPO not provided, yet
31	**Contact details***			Yes	only if DPO not provided, yet
32	**2.3.2 About the contact point where more information can be obtained**				**only if distinct from above**
33	**More information about the incident can be obtained at**	a) DPO b) Reporting person c) Other (please specify)			
34	**Name of the contact person**			Yes, if visible	
35	**Function of the contact person**			Yes, if visible	
36	**Contact details***			Yes, if visible	

Z komentarzem [A7]: The term 'national identification number' suggests that it refers to a number identifying the natural person: the reporting person. We suggest deleting this information. Applications submitted by electronic means require appropriate credentials (e.g. in Poland, login credentials, a trusted profile, etc.), while paper applications bear a handwritten signature. This information therefore appears to be excessive where the applicant's identity is verified by other means.

Z komentarzem [A8]: In what circumstances is this required?

Z komentarzem [A9]: We suggest clarifying that point 34-36 should be supplemented only if the person from whom more information can be obtained is different from the DPO or the notifier.

37	2.4 Involvement of other parties				
38	**Are other parties such as data processors or joint controllers involved?**	a) Yes b) No	Indicate here if other organisations were involved in the data breach (for example a data processor, a joint controller, etc.)	Yes	
39	**Qualification of the other involved party**	For each party: Please specify the role Data Processor, Joint Controller or Other (please describe) and provide identification below		Yes	visible only if "Are other parties such as Data Processors or Joint Controllers involved?" = yes
40	**Name of the other involved party**			Yes	visible only if "Are other parties such as Data Processors or Joint Controllers involved?" = yes Allow multiple
41	**Contact details***			Yes	
42	3. Initial information on the personal data breach				
43	3.1 Date and time of the personal data breach and of its detection				
44	**When did the personal data breach occur?**	a) On a specific day b) From a date to a date c) From a date and is still ongoing d) Cannot be determined e) To be determined	If you do not know the dates precisely, please indicate the estimated dates below	Yes	" f) To be determined" only available for incomplete notification.
45	**Only estimated dates are possible**	[Checkbox]	Please indicated how you estimated the dates of the breach in field 49	No	

Z komentarzem [A10]: Please clarify this identification data: we propose according to the identification data of the reporting entity?

46	**Beginning date and time of personal data breach**			Yes, if visible	
47	**Ending date and time of personal data breach**			Yes, if visible	Only if a,b selected
48	**Date and time of awareness of the data controller of the personal data breach**			Yes	
49	**Reasons for late notification of the personal data breach**			Yes, if visible	Visible only if "date of awareness of breach" + 72h > current time and "new notification"
50	**How was the personal data breach discovered?**	a) Detection by the data controller b) Detection and communication by the data processor c) Communication by a data subject d) Communication by an external party e) Press news f) Other (please specify in further description)		Yes	
51	**Further description of the discovery of the personal data breach**		Please describe how the personal data breach was discovered, e.g., Malware or Intrusions detecion system, Coordinated Vulnerability Disclosure, …	Yes	
52	**Date of notification by other party**		If you do not know this date precisely, please indicate the approximate date.	Yes, if visible	only if external notification (50 is b), c), d), e), f))
53	**Further comments on timeline and additional information**		Please provide an overview over relevant events and other issues regarding the timeline (if applicable), such as, the duration of impacts on availability, integrity and	Yes, if 41a	

Z komentarzem [A11]: We suggest to enter the content of Article 33(1) of the GDPR: after having become aware of it

Z komentarzem [A13]: There is no field 41A. Should it be 44A?

			confidentiality, the awareness date of the processor, etc. Please indicated how you estimated the dates of the breach (if applicable)		
54	3.2 Nature, circumstances and summary of the personal data breach				
55	**Nature of the personal data breach**	a) Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data. b) Integrity breach - where there is an unauthorised or accidental alteration of personal data. c) Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.		Yes	
56	**Type of confidentiality breach**	a) Personal data are exfiltrated or disclosed b) Personal data are likely exfiltrated or disclosed (no evidence) c) Personal data are NOT exfiltrated NOR disclosed (reasonable evidence present) d) Not possible to assess e) To be determined		Yes, if visible	only if confidentiality "To be determined" only available for incomplete notification.
57	**Was the data unintelligible to anyone who was not authorised to access it or were individuals not identifiable?**	a) Yes and protection is still intact (e.g. data was securely encrypted or otherwise protected) b) Protective measures had been taken, but it is likely that they could be subverted (e.g. because the unauthorised party could be able to use decryption keys or exploit a technical weakness in the measures that have been applied) c) No d) Not possible to assess e) To be determined	If you answered d), please specify why the assessment is not possible (e.g. technical reasons)	Yes, if visible	only if confidentiality "To be determined" only available for incomplete notification.
58	**Type of integrity breach**	a) Alteration or modification of the data, with no evidence of illegal or wrong use		Yes, if visible	only if integrity

Z komentarzem [A12]: Please explain the intention.

Z komentarzem [A14]: The text of the GDPR provision refers directly to unauthorized disclosure of, or access to, personal data, so we suggest using the terminology expressly provided for in the GDPR. We assume that at this point the controller will check the appropriate box(es). .We also assume that the controller will select one of the options.

Z komentarzem [A15]: The text of the GDPR provision refers directly to accidental or unlawful alteration, so we suggest using the terminology drawn directly from the provision.

Z komentarzem [A16]: The text of the GDPR provision refers directly to accidental or unlawful destruction (loss), so we suggest using the terminology drawn directly from the provision.

Z komentarzem [A17]: We suggest a negative framing of this criterion, i.e. that, in the absence of evidence to the contrary, access or disclosure cannot be ruled out. In practice, this better reflects the situation that controllers face when most circumstances indicate that no breach occurred, but owing to retention periods the event logs that could definitively confirm this are no longer stored.

Z komentarzem [A18]: We suggest that the EDPB should clarify whether such a case should be classified as a personal data breach, subject to reporting to the supervisory authority, and if so, for what reasons.

Z komentarzem [A19]: Please explain who should assess whether this condition is met, and how such an assessment should be carried out.

		b) Alteration or modification of the data, with evidence of illegal or wrong use, but with the possibility of reversing/recovering the damages to data subjects c) Alteration or modification of the data with evidence of illegal or wrong use, without the possibility of reversing/recovering damages to the data subjects			
59	**Type of availability breach**	a) Temporary availability issue b) Permanent availability issue c) not determined	Please assess the availability issue form the data subject's perspective	Yes, if visible	only if availability
60	**Nature of the incident**	a) Abuse of access privileges by employee b) Encrypted device / ransomware c) Hacking / malware activity detected d) Phishing / social engineering e) Security vulnerability (likely) exploited (known CVE or zero day) f) Unauthorised access to personal data in IT systems g) Data exfiltration / unauthorised extraction of personal data h) Data of wrong data subject shown (mix-up of records) i) Device lost or stolen j) E-waste (personal data still present on obsolete device) k) Incorrect disposal of personal data on paper l) Mail lost or opened / misdelivery (post/email) m) Misconfiguration n) Incorrect access permissions (e.g., cloud storage, shared folder) o) Paper lost or stolen or left in insecure location p) Personal data deleted/destroyed q) Personal data displayed to wrong recipient		Yes	

Z komentarzem [A20]: What situations does this cover? Could you point to some examples? Is this a corrective action?

Z komentarzem [A21]: What situations does this cover? Could you point to some examples? Is this a corrective action?

Z komentarzem [A22]: These categories are not mutually exclusive (e.g. abuse of permissions can lead to unauthorized access). We suggest clarifying whether controllers should be able to check several boxes at once, or whether these categories are intended to be mutually exclusive

		r) Personal data sent by mistake (post/email) s) Sending email to multiple recipients without blind copy / with open distribution list t) Technical malfunction u) Unauthorised data modification v) Unintended publication (e.g., public link / public website / shared drive) w) Verbal unauthorised disclosure of personal data x) to be determined y) Other (please specify in further description)			
61	**Cause of the personal data breach**	a) Internal non malicious b) Internal malicious c) External non malicious d) External malicious e) To be determined f) Unknown		Yes	"To be determined" only available for incomplete notification.
62	**Further description of the nature of the incident**		Please describe the nature of the breach (detection, awareness, cause, measures in place) shortly and provide on what facts your decision is grounded. If possible indicate the root cause of the incident.	Yes	
63	**Description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located**		Please list the descriptions them in semantic groups, e.g. Systems: • production database : o client database (full/partial) that countains ****, located in *** o internal HR database (full/partial) that countains ****, located in ***	Yes	

Z komentarzem [A23]: Does not malicious / malicious equal to unintentional / intentional?

Z komentarzem [A24]: To what does this decision relate: the level of risk, or the remedial measures taken?

Z komentarzem [A25]: What does 'location' mean in this context? Not every breach affects a system or database. A breach may, for instance, be caused by a courier company losing a shipment. Most breaches do not concern IT systems but result from human error. We suggest this could be an optional field rather than a mandatory one.

			• test infrastucture o testing database (full/partial) that countains ****; located in *** Software: • Accounting software • Payment system software		
64	3.3 Categories and number of data subjects concerned				
65	**Categories of concerned data subjects**	a) Customers (current and prospects) b) Employees (former, current and candidates) c) Military or law enforcement staff d) Minors e) Patients f) Students g) Subscribers h) Users i) Vulnerable individuals (elderly, refugees, disabled people, victims, …) j) Additional concerned data subjects (please specify in further description) k) Not yet known	If you answered i), please indicate what kind of vulnerable people. If you are not sure if or how the concerned data subject are vulnerable, please describe them shortly and why you would consider them as vulnerable.	Yes	”Not yet known” only available for incomplete notification.
66	**Further description of categories of concerned data subjects and additional data subjects**			Yes	
67	**Data subjects concerned by the personal data breach**	a) Exact number b) Approximate number c) Number cannot be determined		Yes	”Number to be determined ” only available for

		d) Number to be determined			incomplete notification.
68	**Number of data subjects concerned by the personal data breach**			Yes, if 'exact number' or 'approximate number' in previous question	Only if a/b selected ask according to selected value before, Tooltip: "if c) the current estimate is: …"
69	3.4 Categories and number of personal data records concerned				
70	**Type of breached data**	a) Basic data (e.g. name, surname, date of birth) b) Contact details (e.g. address, phone number, e-mail) c) Biometric data d) Criminal convictions, offence or security measures e) Data revealing political opinions f) Data revealing racial or ethnic origin g) Data revealing religious or philosophical beliefs h) Data revealing sex life or sexual orientation i) Data revealing trade union membership j) Genetic data k) Health data (e.g. medical records, test results, …) l) Economic and financial data m) Employment related health data (e.g. proof of sick leave, proof of medical attendance, results of medical fitness tests or similar) n) Identification data (e.g. National identification number, ID number) o) Location data		Yes	"Not yet known" only available for incomplete notification.

Z komentarzem [A26]: Will the answer to this question always be the same as answer 67 a or 67b?

Z komentarzem [A27]: Will this be a multiple-choice field? Our experience to date indicates that the scope of the compromised data typically falls under at least two of the listed options.

Z komentarzem [A28]: For the purpose of the unique identification of a natural person

		p) Official documents (e.g. scanned copies) q) Payment methods (e.g. credit card, bank accounts) r) Profile data (e.g. social network, credit score, psychology or other profiles) s) User credentials (e.g. usernames, passwords, tokens) t) Not yet known u) Additional data types (please specify in further description)			
71	**Further description of breached data and additional data categories**			Yes	
72	**Personal data records concerned by the personal data breach**	a) Exact number b) Approximate number c) Number cannot be determined d) Number to be determined	Please specify the type of record: number of data about each concerned data subject. For instance, to avoid just mentionning “500”. Because “5 types of data (namely *,*,*,*,*) about 100 people” and “100 types of data (namely *,*,*,*,*) about 5 people” may not lead to the same risks assessment, even if it could both be sumed up to “500 records”.	Yes	”Number to be determined ” only available for incomplete notification.
73	**Number of personal data records concerned by the personal data breach**		Please indicate here the number of records concerned by the breach, meaning the number of single entries in the database concerned by the breach.	Yes	ask according to selected value before
74	3.5 Measures in place when the personal data breach occurred				
75	**Relevant measures in place when the personal data breach occurred**	a) Pseudonymisation b) Backup / Recovery plan c) Data encryption d) Data protection and information security policies	This list is not exhaustive and just covers common measures.	Yes	

Z komentarzem [A29]: Please explain what these categories (indicated in point 70) of data are based on. This approach raises concerns because the categories are not mutually exclusive (e.g. economic and financial data may include payment method data, and profile data, such as a creditworthiness assessment, may include financial data). We suggest including only mutually exclusive categories, so that the same type of information is not described in several different ways

Z komentarzem [A30]: What does this mean? For instance, when assessing the breach that result in the loss of 5 invoices, should a single invoice be treated as 1 record , or should each category of data contained in the invoice (e.g. name) be counted as separate record? The latter option significantly increases the handling time of the call, for which telecommunications companies have 24 hours.
Please provide an explanation of what should be understood by the record, i.e. whether it is indeed one invoice or every information that is on it. Alternatively, the form should contain a space for the controller’s comment, in which it will be able to explain what is meant by the entry in a given violation.

		e) Data protection and security training f) Incident log g) Levels of access to data h) Logical access control (e.g. MFA) i) Periodic audits j) Physical access control k) Up-to-date IT systems l) Other measures (please specify in further description)	You may have not applied some measures because they were not applicables or useful. At the same time, you may have applied non-listed measures that were useful. If so, please specify them with answer L.		
76	**Further description of relevant measures in place when the personal data breach occurred**		Reminder: You indicated that technical measures are likely to be subverted by the adversaries. Please add the relevant level of detail here to these measures, along the description of the other relevant measures.	Yes	If 57 indicated that measures in place are likely to be subverted, remind DCs here to detail on this in the tooltip
77	4. Further information on the personal data breach				
78	4.1 Likely consequences of the personal data breach and potential adverse effects on data subjects				
79	**Likely consequences in case of breach of confidentiality**	a) Data were disclosed beyond the scope of the privacy policy or relevant legislation b) Data may be linked, without unreasonable effort, with other information regarding data subjects c) Data may be used for purposes other than the intended purpose or unlawfully d) Other e) Under assessment		Yes, if visible	visible only if "Confidentiality"= yes "Under assessment " only available for incomplete notification.
80	**Description of other confidentiality consequences**			Yes, if visible	visible only if "Other" = Yes

Z komentarzem [A31]: As the EDPB rightly pointed out, any such list is an open-ended catalogue. At the same time, under the current approach, controllers may have difficulty deciding whether to select a specific measure. For example, if a breach affects a system made up of separate functionalities and databases, it may turn out that the controller has set access levels for the individual databases, but that within the system itself all roles are identical. In such a case, some controllers might indicate that they use this measure and others that they do not. We therefore suggest that this field be completed entirely by controllers themselves (without a general sample list)

81	**Likely consequences in case of breach of integrity**	a) Data may have been modified and used even though it is no longer valid b) Data may have been modified into otherwise valid data and subsequently used for other purposes c) Other d) Under assessment		Yes, if visible	visible only if "Integrity"= 1 ”Under assessment ” only available for incomplete notification.
82	**Description of other integrity consequences**			Yes, if visible	visible only if "Other" = Yes
83	**Likely consequences in case of breach of availability**	a) Inability to access services b) Service disruptions and difficulties in service use c) Other d) Under assessment		Yes, if visible	visible only if "Integrity"= 1 ”Under assessment ” only available for incomplete notification.
84	**Description of other availability consequences**			Yes, if visible	visible only if "Other" = Yes
85	**Nature of the potential impact for the data subject**	a) Loss of control of their personal data b) Limitation of their rights c) Discrimination d) Identity theft or usurpation e) Fraud f) Financial loss g) Unauthorised reversal of pseudonymisation h) Damage to reputation i) Loss of confidentiality of personal data protected by professional secrecy j) Disclosure of data to unauthorised third parties k) Significant economic or social disadvantage l) Physical or mental harm m) Material or non-material damage to property n) Other impact (please specify in further description) o) To be determined	Please indicate here the nature of the impact on the data subject rights and freedoms.	Yes	
86	**Further description of the other impacts for the data subjects**			Yes, if visible	visible only if "Description of the potential impact

					for the data subject" = "other"
87	**Severity of the potential impacts**	a) Minor b) Moderate c) Severe d) To be determined	Indicate here the result of your self-assessment of the severity of the impact of the breach for the data subjects. Please select the highest severity if multiple potential impacts can occur.	Yes	
88	4.2 Assessment of the risk to the rights and freedoms of natural persons				
89	**Outcome of the risk assessment carried out by the controller**	a) The personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons b) The personal data breach is likely to result in **a (not high) risk** to the rights and freedoms of natural persons c) The personal data breach is **unlikely to result in a risk** to the rights and freedoms of natural persons c) Additional information is needed to assess the risk to the rights and freedoms of natural persons		Yes	”Additional information is needed to assess the risk to the rights and freedoms of natural persons ” only available for incomplete notification.
90	**Further description of the risk assessment carried out by the data controller**		Please describe the metodology used and the relevant factors you put into account.	Yes	
91	4.3 Measures taken (or proposed to be taken) to address the personal data breach and to mitigate its possible adverse effects				
92	**Measures taken to address the personal data breach and to mitigate its consequences**		Please indicate to what extend the measures resolve the issue.	Yes	
93	4.4 Measures taken (or proposed to be taken) to prevent similar personal data breach				

Z komentarzem [A32]: The GDPR uses the concept of a risk to the rights and freedoms of data subjects. A risk assessment consists of assessing both the severity of the infringement and its likelihood. We suggest considering whether it is appropriate to treat the severity criterion both separately and as part of the overall risk assessment. If so, we suggest that controllers be given guidance on how to select the methodology they should use to assess the severity of the breach

Z komentarzem [A34]: According to Art. 33 GDPR, such cases are not subject to mandatory notification - we suggest that this information be included in the form.

Z komentarzem [A33]: The document should include the recommended risk assessment method

94	**Relevant measures taken to prevent similar personal data breach**	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 o) Other measures (please specify in further description)		Yes	
95	**Further description of relevant updated permanent measures to avoid similar incidents in the future**		Please indicate to what extend the measures resolve the issue and improve the situation. A description is **expected** if you answered with “Other measures” in the previous question m). Nevertheless, do not hesitate to describe further measures taken after the breach, or to be taken, if you think it is relevant.	Yes	

Z komentarzem [A35]: Note similar to paragraph 75.

96	5. Communication to the data subjects				
97	**Has the personal data breach been communicated to data subjects?**	a) Yes b) No, but it will be communicated on a specific date b1) No, but it will be communicated on a date to be determined c) No, the investigation is still ongoing d) No, it will not be communicated since the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons e) No, it will not be communicated since one of the conditions referred to in article 34(3) of the GDPR is met	If you have not assessed yet if you are going to notify, please note that you will have to make a follow-up notification once you have make your decision If you communicate the data breach to the data subjects in phases or if you cannot reach out to all data subjects, yet. Please indicated that in field 98 and 98a.	Yes	No, the risk assessment is still ongoing' only available for incomplete notifications.
98	**Date of when information was given to data subjects**		Please indicate here the date on which you have started to inform the data subjects.	Yes, if visible	visible only if "information of data subject" = Yes
99	**Future date on which the data breach will be communicated to the data subjects**			One of the fields is mandatory if "information of data subject" = "No, but it will be communicated"	visible only if "information of data subject" = "No, but it will be communicated"
100	**Further information about conditions referred to in article 34(3) of the GDPR that are met**	a) The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption. b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise. c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or		Yes, if visible	visible only if "information of data subject" = "No they will not be informed"

		similar measure whereby the data subjects are informed in an equally effective manner.			
101	**Further description why the conditions referred to in article 34(3) of the GDPR that are met and the measures taken**			Yes, if visible	visible only if "information of data subject" = "No they will not be informed"
102	**Number of data subjects informed**	a) All data subjects have been informed b) Not all data subjects have been informed		Yes, if visible	visible only if "information of data subject" = Yes
103	**Further description why not all data subjects have been informed**		Please specify the reason why some data subjects have not been informed, e.g. some might not have been because reason A, some other because reason B, etc. Reasons can be of various natures and not just the technical ones have to be considered: ongoing process, some data subjects cannot be reached the same way, additionnal laws apply to them, the cost of information is much higher, etc	Yes, if visible	visible only if "b) Not all data subjects have been informed"
104	**Means of communication used to inform the data subject**	a) Individual communication (letter/email/personal communication) b) Public announcement (website/press release/social network) c) Other		Yes, if visible	visible only if "information of data subject" = Yes
105	**Further description of the other means of communication**			No	visible only if "information of data subject" = Yes
106	**Content of the information provided to the data subjects**		Please provide this content in the most relevant way. For example, if the provided information is just an email	Yes, if visible	visible only if "information of

			with only plaintext, copying the text here is sufficent. If, for instance, your information contains pictures/videos useful for understanding, please provide the means for the data protection authority to consult it (website page, email screenshots, download page, etc).		data subject" = Yes
107	6. Possible other issues				
108	6.1 Whether other authorities or bodies have been notified				
109	**Has the incident been reported to the police/judicial authorities as a criminal offence?**	a) Yes b) No c) Unknown		No	
110	**Has the incident been notified to other supervisory authorities or control bodies under other relevant legislation? (e.g. national cyber security centre, etc.)**	a) Yes b) No c) Unknown		No	
111	**Further information about notification to other authorities or bodies**		Please specify which authority (about data protection or not) and if possible, provide the case ID that this authority used and then can be referred to.	Yes, if visible	visible only if 109/110 is Yes
112	6.2 Whether the personal data breach involves a cross-border processing				
113	**Does the personal data breach involve cross-border processing carried**	a) Yes b) No c) Unknown		Yes	**SECTION:** Only if DC is based in EEA

Z komentarzem [A36]: Coordination with NIS2.
At the same time, we suggest that, in paragraphs 109 and 110, it should be possible to indicate that this matter is still being determined.

	out by a controller established in the European Economic Area (EEA)?				
114	**The lead supervisory authority is:**	List of SAs/unknown		Yes, if visible	
115	**List of EEA countries where the controller has an establishment**	List of EEA countries BE;BG;DK;DE;EE;FI;FR;GR;IE;IT;HR;LV;LT;LU;MT;NL;AT;PL;PT;RO;SE;SK;SI;ES;CZ;HU;CY;IS;LI;NO	Indicate here the countries concerned by the breach.	Yes, if visible	visible only if "Is this notification a cross border notification made to your lead supervisory authority" = Yes
116	**List of EEA countries where affected data subjects are located**	List of EEA countries BE;BG;DK;DE;EE;FI;FR;GR;IE;IT;HR;LV;LT;LU;MT;NL;AT;PL;PT;RO;SE;SK;SI;ES;CZ;HU;CY;IS;LI;NO	Indicate here the countries concerned by the breach.	Yes, if visible	visible only if "Is this notification a cross border notification made to your lead supervisory authority" = Yes
117	**Approximate number of data subjects per country**	Ask number for each affected country		Yes, if visible	Only for selected countries
118	**List of EEA supervisory authority to which the breach has been or will be notified**	Austria - Datenschutzbehörde Austria - Parlamentarisches Datenschutzkomitee Belgium - Autorité de protection des données / Gegevensbeschermingsautoriteit Bulgaria - Комисия за защита на личните данни Cyprus - Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Croatia - Agencija za zaštitu osobnih podataka Czech Republic - Úřad pro ochranu osobních údajů Denmark - Datatilsynet Estonia - Andmekaitse Inspektsioon	Indicate here the list of other EU Supervisory Authorities you have or you plan to notify.	Yes, if visible	

		Finland - Tietosuojavaltuutetun Toimisto / Dataombudsmannens Byrå France - Commission Nationale de l'Informatique et des Libertés Germany (Federal) - Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Germany (Baden-Württemberg) - Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg Germany (Bavaria - Private sector) - Bayerisches Landesamt für Datenschutzaufsicht Germany (Bavaria - Public sector) - Der Bayerische Landesbeauftragte für den Datenschutz Germany (Berlin) - Berliner Beauftragte für Datenschutz und Informationsfreiheit Germany (Brandenburg) - Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg Germany (Bremen) - Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Germany (Hamburg) - Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Germany (Hesse) - Hessische Beauftragte für Datenschutz und Informationsfreiheit Germany (Lower Saxony) - Der Landesbeauftragte für den Datenschutz Niedersachsen Germany (Mecklenburg-Western Pomerania) - Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Germany (North Rhine-Westphalia) - Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen			

		Germany (Rhineland-Palatinate) - Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz Germany (Saarland) - Unabhängiges Datenschutzzentrum Saarland / Landesbeauftragte für Datenschutz und Informationsfreiheit Germany (Saxony) - Sächsische Datenschutz- und Transparenzbeauftragte Germany (Saxony -Anhalt) - Landesbeauftragte für den Datenschutz Sachsen-Anhalt Germany (Schleswig-Holstein) - Landesbeauftragte für Datenschutz Schleswig-Holstein / Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Germany (Thuringia) - Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Greece - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Hungary - Nemzeti Adatvédelmi és Információszabadság Hatóság Iceland - Persónuvernd Ireland - Data Protection Commission / An Comisiún um Chosaint Sonraí Italy - Garante per la protezione dei dati personali Latvia - Datu valsts inspekcija Liechtenstein - Datenschutzstelle Lithuania - Valstybinė duomenų apsaugos inspekcija Lithuania - Žurnalistų etikos inspektoriaus tarnyba Luxembourg - Commission Nationale pour la Protection des Données / Nationale Kommission für Datenschutz Großherzogtum Malta - Office of the Information and Data Protection Commissioner Norway – Datatilsynet			

		The Netherlands - Autoriteit Persoonsgegevens Poland - Urząd Ochrony Danych Osobowych Portugal - Comissão Nacional de Proteção de Dados Romania - Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal Slovakia - Úrad na ochranu osobných údajov Slovenskej republiky Slovenia - Informacijski pooblaščenec Spain - Agencia Española de Protección de Datos Sweden - Integritetsskyddsmyndigheten			
119	6.3 Whether the personal data breach involves a processing at non-EU establishments				
120	**Does the personal data breach involve processing, to which the GDPR applies, carried out by a controller that is not established in the European Economic Area (EEA)?**	a) Yes b) No c) Unknown		Yes	**SECTION:** Only if DC is NOT based in EEA
121	**List of EEA countries where affected data subjects are located**	List of EEA countries BE;BG;DK;DE;EE;FI;FR;GR;IE;IT;HR;LV;LT;LU;MT;NL;AT;PL;PT;RO;SE;SK;SI;ES;CZ;HU;CY;IS;LI;NO	Indicate here the countries concerned by the breach.	Yes, if visible	only if yes on first
122	**Approximate number of data subjects per country**	Ask number for each affected country		Yes, if visible	only if yes on first only for selected countries
123	**List of EAA supervisory authority to which the breach has been or will be notified**	Austria - Datenschutzbehörde Austria - Parlamentarisches Datenschutzkomitee Belgium - Autorité de protection des données / Gegevensbeschermingsautoriteit Bulgaria - Комисия за защита на личните данни	Indicate here the list of other EU Supervisory Authorities you have or you plan to notify.	Yes, if visible	only if yes on first

		Cyprus - Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Croatia - Agencija za zaštitu osobnih podataka Czech Republic - Úřad pro ochranu osobních údajů Denmark - Datatilsynet Estonia - Andmekaitse Inspektsioon Finland - Tietosuojavaltuutetun Toimisto / Dataombudsmannens Byrå France - Commission Nationale de l'Informatique et des Libertés Germany (Federal) - Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Germany (Baden-Württemberg) - Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg Germany (Bavaria - Private sector) - Bayerisches Landesamt für Datenschutzaufsicht Germany (Bavaria - Public sector) - Der Bayerische Landesbeauftragte für den Datenschutz Germany (Berlin) - Berliner Beauftragte für Datenschutz und Informationsfreiheit Germany (Brandenburg) - Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg Germany (Bremen) - Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Germany (Hamburg) - Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Germany (Hesse) - Hessische Beauftragte für Datenschutz und Informationsfreiheit Germany (Lower Saxony) - Der Landesbeauftragte für den Datenschutz Niedersachsen			

		Germany (Mecklenburg-Western Pomerania) - Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Germany (North Rhine-Westphalia) - Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Germany (Rhineland-Palatinate) - Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz Germany (Saarland) - Unabhängiges Datenschutzzentrum Saarland / Landesbeauftragte für Datenschutz und Informationsfreiheit Germany (Saxony) - Sächsische Datenschutz- und Transparenzbeauftragte Germany (Saxony -Anhalt) - Landesbeauftragte für den Datenschutz Sachsen-Anhalt Germany (Schleswig-Holstein) - Landesbeauftragte für Datenschutz Schleswig-Holstein / Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Germany (Thuringia) - Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Greece - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Hungary - Nemzeti Adatvédelmi és Információszabadság Hatóság Iceland - Persónuvernd Ireland - Data Protection Commission / An Comisiún um Chosaint Sonraí Italy - Garante per la protezione dei dati personali Latvia - Datu valsts inspekcija Liechtenstein - Datenschutzstelle Lithuania - Valstybinė duomenų apsaugos inspekcija Lithuania - Žurnalistų etikos inspektoriaus tarnyba			

		Luxembourg - Commission Nationale pour la Protection des Données / Nationale Kommission für Datenschutz Großherzogtum Malta - Office of the Information and Data Protection Commissioner Norway – Datatilsynet The Netherlands - Autoriteit Persoonsgegevens Poland - Urząd Ochrony Danych Osobowych Portugal - Comissão Nacional de Proteção de Dados Romania - Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal Slovakia - Úrad na ochranu osobných údajov Slovenskej republiky Slovenia - Informacijski pooblaščenec Spain - Agencia Española de Protección de Datos Sweden - Integritetsskyddsmyndigheten			
124	7. Attachments				
125	**Please identify the attachments to this notification**	a) Dated copy of the communication to the datasubject b) Dated copy of the risk-assessment c) Dated copy of the research report into the data breach (cyberincidents) d) Dated copy of the ransomware-note e) Dated copy of the phishing-message f) Dated copy of the internal procedure to notify a data breach g) Dated copy of the internal policy to delete/destroy (outdated) personal data	Tooltip: with regard to *phishing* there needs to be a split-up of communications, namely, 3 categories: - The owner, datasubject of the mailbox - Data subjects that received a phishing-mail - Data subjects of which personal data was in the compromised mailbox	No	

Z komentarzem [A38]: This field should be optional or removed, since various types of evidence may be generated in the course of handling each breach. At the same time, if the field is retained but controllers do not upload any attachments, will the authorities call on controllers to supply these documents? If this field were mandatory, it would complicate and prolong the reporting time for each breach

		h) Dated copy of the communication to the wrong recipients i) Dated copy of the external notification/message of the data breach j) Other			
126	**Other attachements**			Yes, if visible	

* Marks simplified Fields for easier reading. The collection in the actual form shall be in a structured way.

For the European Data Protection Board

The Chair

Anu Talus

Z komentarzem [A37]: We suggest clarifying this so that controllers send only a communication requesting the deletion of a message received in error, addressed to the unauthorized recipient. The current wording may suggest that controllers should forward the original erroneous messages themselves, which could cause further data protection breaches

Polish Telecommunication and Information Technology Chamber General Conclusions and Comments on Template for personal data breach notification

Statement of facts concerning the form

Article 33(3) of the GDPR provides for the following scope of notification:

3. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

For Regulation 611/2013, it is:

ANNEX I

Content of the notification to the competent national authority

Section 1

Identification of the provider

1. Name of the provider

2. Identity and contact details of the data protection officer or other contact point where more information can be obtained

3. Whether it concerns a first or second notification

Initial information on the personal data breach (for completion in later notifications, where applicable)

4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident

5. Circumstances of the personal data breach (e.g. loss, theft, copying)

6. Nature and content of the personal data concerned

7. Technical and organisational measures applied (or to be applied) by the provider to the affected personal data

8. Relevant use of other providers (where applicable)

Section 2

Further information on the personal data breach

9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):

10. Number of subscribers or individuals concerned

11. Potential consequences and potential adverse effects on subscribers or individuals

12. Technical and organisational measures taken by the provider to mitigate potential adverse effects

Possible additional notification to subscribers or individuals

13. Content of notification

14. Means of communication used

15. Number of subscribers or individuals notified

Possible cross-border issues

16. Personal data breach involving subscribers or individuals in other Member States

17. Notification of other competent national authorities

Overall assessment of the form

Overall, the analysis of the proposed content for the personal data breach notification form points to a clear conclusion: the form is a single 127-row table comprising 107 fields, organized into 7 main sections and roughly 20 subsections, what causes it to generate bureaucratic burden

These fields break down as follows:

42 mandatory fields ("Yes")

45 conditional fields ("Yes, if applicable / if visible")

10 optional fields ("No")

In practice, this means more than half the form consists of conditions and business logic that notifiers must work through to determine what applies to them and whether a given field needs to be completed. A structure of this kind leaves notifiers with the impression that the form is too long, too time-consuming, and too difficult.

Furthermore, we would like to share our observations:

1. **Disproportionate detail in identifying the notifier.** Section 2 (identification) contains roughly 30 fields, more than the entire description of the breach itself. Subsection 2.2, "Identity of the reporting person," alone has 16 fields, duplicating data across the reporting person, the DPO, and the "contact point." For notifications due within 24 hours (e.g., telecoms) or 72 hours (other entities), these proportions are inverted: the general administrative section outweighs the substance of the breach.
2. **Excessive fields of low informational value**, Fields such as "Classification of economic activity" (with a full list of PKD/NACE sections A–V), "Type of organization," "Sector," and "Further description of organization type" are essentially statistical data, irrelevant to risk assessment, and

they lengthen and complicate completion of the form. It is worth proposing that such fields be made purely optional, populated automatically from registers, or removed altogether.

3. **Redundant time and descriptive fields.** Section 3.1 devotes 10 fields to chronology alone (start, end, detection, reason for delay, "further description of discovery," "further remarks on timeline"). Several overlap substantively; we recommend consolidating them into a single descriptive field plus dates.
4. **Structural flaws.** Headings 2.3, 2.3.1, and 2.3.2 are nested within section 2.2 rather than forming their own levels, and the table layout mixes headings with data fields. This genuinely hinders navigation and should be flagged as a broader problem with the document's clarity.
5. **No proportionality test against the governing provision (Article 33(3) GDPR).** Article 33 requires only a minimum: the nature of the breach, DPO contact details, likely consequences, and measures taken. The form goes well beyond this closed list. The key point is that the template significantly expands the scope of the information obligation beyond the wording of the provision, shifting onto the controller the burden of completing fields the GDPR does not require. To illustrate the position for telecoms operators, I have inserted the text of the annex to Regulation 611/2013 at the top.
6. **The expectation that notifiers attach a large volume of documents and correspondence at the reporting stage**, e.g., exchanges with the reporting person or affected individuals, or notes on an attack — should be regarded as counterproductive. At this stage the controller should be focused on quickly verifying the causes of the incident and minimizing its effects on individuals, not on generating extensive paperwork simply to file the notification.

Conclusions

Completing the form in its proposed shape within 24 hours (for electronic communications operators) or 72 hours, as one element of documenting a personal data breach, is an unrealistic expectation for many entities, and one that does not, in practice, serve to protect the rights and freedoms of the affected individual. In real terms, it may require deploying multi-person teams solely to fill out this form.

1. We view positively the idea of a uniform breach notification form for the national data protection authority, and especially the option of submitting it online through the DPA's system, including the UODO. This, at least, is how we understand the direction of the work underway.
2. The template defines a data model for exchanging breach notifications between supervisory authorities. Under the GDPR's comprehensive cooperation mechanism, notifications concerning cross-border processing circulate among authorities through the IMI system. This constitutes a "trans-European digital service" within the meaning of Regulation 2024/903 (recital 6: cross-border data exchange between public sector bodies). We therefore submit that work on such templates should proceed from the outset with interoperability requirements in mind, and with the involvement of the ministers responsible for digitalizing public administration across EU member states. Otherwise, we risk additional difficulties and costs when integrating the template into DPA IT systems and enabling data exchange between them.

At a minimum, the EDPB should carry out an interoperability assessment, involve the Interoperable Europe Board together with the national competent authorities and interoperability coordinators, and align the template with the European Interoperability Framework (its legal, organizational, semantic, and technical layers).

As a preliminary matter, based on the template's current content, we have identified the following interoperability issues to be resolved.

Legal Layer

1. Field 25 (national identification number, "implement only if required") rests on different legal bases across countries. Even within Poland the practice is inconsistent — REGON, NIP, PESEL. At the EU level, the BRIS identifier (the KRS number prefixed with "PL") is also relevant for companies. It is unclear whether the comment refers to a national legal requirement to provide a specific type of identification number. In any event, this will pose a challenge for data exchange at the EU, supranational level.
2. Row 111 (read together with rows 109–110) concerns notifications to other authorities (e.g., a national CSIRT). This overlaps with reporting obligations under NIS2 and DORA, yet the content and descriptions provide no mapping to those regimes.

Organizational Layer

In implementing the one-stop-shop approach, DPAs use the EU's IMI system on a pilot basis (the GDPR is not listed in the annex to Regulation 1024/2012). IMI is the tool that gives practical effect to Article 60 (cooperation between the lead authority and the authorities concerned, and the exchange of "all relevant information"), Article 61 (mutual assistance), Article 62 (joint operations), and Article 64 (consistency mechanism) of the GDPR; Article 67, in turn, empowers the Commission to adopt implementing acts specifying the electronic exchange of information and a standard format. The template must connect the notification to the national reception point with the IMI- and GDPR-based exchange of data between authorities.

Semantic layer

This is where the greatest risk lies. Vocabularies are the principal resource for interoperability: the nature of the incident (field 60, items a–y), the types of data breached (field 70), and the classification of activity (field 17, similar to NACE). The content declares no link to existing EU vocabularies (EU Vocabularies, Core Vocabularies, NACE codes, ISO). Identifiers of authorities and countries should be consistent, and translations of vocabulary values into EU languages must preserve identical meaning.

Moreover, because this is a notification to a national authority, it must accommodate all official languages and legally required forms of communication in the country concerned. In Poland this includes PJM (Polish Sign Language): a notification submitted in PJM by a Deaf person is legally permissible, indeed a recognized entitlement, and the public authority is bound to accept it in that form. The legally permissible forms of communication between citizens and a given DPA must be supported by that DPA's IT system and must be given an interoperable designation for the purposes of Regulation 2024/903. Finally, there is no common identifier scheme to link a single breach across systems (fields 6, 7, and 111).

Technical Layer

The document states that data collection should be "structured." If so, work on a machine-readable schema (XSD/JSON Schema), though not necessarily on a full API specification, should begin from the outset, in parallel with discussions on the form's content. The interoperability regulation requires an open data model and an API. Without a published schema, each authority will build its own implementation (field types, formats, encoding). Conditional logic expressed in prose is not executable; it needs to be formalized. And there is no provision for versioning (v1.0) or for version negotiation between systems.

In short: before the EDPB finalizes the template, an interoperability assessment under Article 3 of Regulation 2024/903 should be carried out, and the template should be coordinated with the Interoperable Europe Board, considering the processes handled in IMI for DPAs. A machine-readable schema should be published, and the vocabulary should be linked to EU Vocabularies, NACE, and ISO.

1. **Editorial note regarding rows 118 and 123.** In Poland, the data protection authority is the President of the Personal Data Protection Office (PUODO). Poland's notification to Article 51 of the GDPR is correct (attached).

Please see below for further suggestions.

No.	Row / Section	Content of Comment	Proposed Change
1	Entire form (107 fields)	The form contains 107 fields, of which only 42 are strictly mandatory, 45 conditional, and 10 optional. The conditional and statistical layers overshadow the informational scope actually required by Article 33(3) GDPR and Regulation 611/2013, making the form excessively long and difficult to complete within the 24-hour or 72-hour regime.	Clearly separate the essential information required by Article 33 GDPR or Regulation 611/2013 from the optional and statistical layer; the latter should be deleted, hidden by default, or marked as non-mandatory.
2	Entire form	The scope of information requested goes beyond the closed enumeration in Article 33(3) GDPR (the nature of the breach, DPO contact details, likely consequences, and measures taken). The template shifts onto the controller the burden of completing fields the provision does not require. Details about the entity's structure and the like add nothing to the essence of the matter, which is establishing that a breach has occurred	Limit the mandatory fields to the content of Article 33(3) GDPR (and Regulation 611/2013); delete the remaining fields or mark them as optional, or as information to be supplied in phases through a supplementary notification where required.
3	14–17	The fields "Sector," "Type of organization," "Further description of organization type," and "Classification of economic activity" (the full list of sections A–V) are statistical data irrelevant to risk assessment, and they significantly lengthen and complicate completion of the form	Mark them as fully optional, retrieve them automatically from official registers on the basis of an identifier, or remove them entirely (rows 10–11).
4	20–36 (2.2 and 2.3)	The identity sections comprise 16 fields and collect similar data three times over, for the reporting person, the Data Protection Officer, and the "contact point", which leads to duplication of the same contact details.	Consolidate these into a single "person / contact point" block, with the option to designate the DPO as the default contact, and remove the duplicated "Contact details" fields.

No.	Row / Section	Content of Comment	Proposed Change
5	26	The label "Accuracy and responsibility" is unclear. It is not apparent what information the field is meant to capture.	Clarify the purpose of the field and correct its name; if it concerns a declaration that the notification is correct, say so directly in the label.
6	44–53 (3.1)	The section devotes 10 fields to the chronology of the event. The fields "Further description of breach discovery" (51) and "Further remarks on timeline and additional information" (53) overlap substantively.	Consolidate the descriptive fields (51 and 53) into a single free-text field, and retain only the dates as structured fields.
7	53	The mandatory condition reads "Yes, if 41a" and points to a designation that does not exist or is unclear. This prevents the conditional logic from being applied correctly.	Correct the reference to point to the appropriate row or condition, or remove the faulty rule..
8	55–63 (3.2)	Breaking this out into separate fields: "Type of confidentiality / integrity / availability breach," together with "Further description of the nature of the incident" and "Description of systems, software, services, and infrastructure" creates excessive granularity at the initial stage.	Combine the descriptive fields, and move the description of systems and infrastructure to a supplementary notification.
9	63	The field "Description of systems, software, services, and infrastructure" is marked as mandatory ("Yes"), yet at the initial notification stage (24 or 72 hours) the technical details are often not yet established. Moreover, some breaches will not involve any systems or applications at all — for example, the loss of a courier shipment.	Reclassify the field as conditional ("if applicable"), or assign it to a supplementary notification.
10	79–86 (4.1)	This section reproduces the three-way confidentiality / integrity / availability split across six fields ("likely consequences" plus "description of other consequences," ×3), which triples the same structure and lengthens the form.	Reduce this to one field for selecting the consequences (multiple choice across C-I-A) and one free-text description field.

No.	Row / Section	Content of Comment	Proposed Change
11	98–99	The condition in row 99 ("One of the fields is mandatory") does not clearly indicate its relationship to row 98 (date the information was provided vs. a future date). The "either/or" rule is imprecise.	Clarify the exclusive logic between rows 98 and 99 (exactly one of the fields is to be completed)
12	112–123 (6.2 and 6.3)	The cross-border section (6.2) and the "outside EU" section (6.3) duplicate the same fields: a list of EEA countries, the approximate number of persons by country, and a list of supervisory authorities. This means entering similar data twice.	Merge these into a single cross-border section with one set of fields and a "processing outside the EU: yes / no" toggle.
13	123	The abbreviation "EAA" is used ("supervisory authorities of the EAA"), whereas the correct term used throughout the document is EEA (cf. row 18). This inconsistency creates confusion about the geographical scope.	Standardize on "EEA" throughout the document.
14	27, 28, 32	Headings 2.3, 2.3.1, and 2.3.2 are embedded as data rows within section 2.2 instead of forming separate levels in the hierarchy. This hinders navigation and blurs the form's structure.	Extract 2.3 as an independent section with the correct heading level, and regularize the numbering.
15	Attachments	The section contains a number of attachments.	Remove the entire section. Documented evidence of this kind can be, and in practice is, requested by the supervisory authority during proceedings.