

Template [2026] for personal data breach notification

Version 1.0

Adopted on 08 June 2026

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" =

					"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	

		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	

Commenté [A1]: It could be broader.
For example: reporting person could be a vendor (processor).

In the clinical research sector, data breach is often shared by vendors who processes in practice the data.

		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	

Commenté [A2]: Which kind of information is subjet here ?

Is it information to the data subject ? To detemrine who is responsible for the potential notification ?

Commenté [A3]: Proposition:
Adding of DPR

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	

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	

			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

		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	

		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	

			• 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.

		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	

		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

Commenté [A4]: From a professional perspective, the appreciation of those criteria is too vague.

It would be helpful if the EDPB could provide an objective grid of evaluation helping to estimate when there is high risk.

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				

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	

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

	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	

		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