Clusit welcomes the initiative of defining a unified template for personal data breach notification to be implemented by DPAs via an IT tool. Uniform personal data breach notification among Member States could help provide a common and comparable view of data breaches. From a market perspective, Data Controllers are increasingly using IT tools to deal with different regulatory requirements, and a unified template may help introduce tools that can be effectively used among the different Member States. Also, corporate groups operating in different Member States may need to notify data breaches to different authorities, and a unified template may help in reducing the complexity of this activity. However, it is not clear from the information provided wether DPAs will be required (or at least strongly encouraged) to adopt this template, or it will just be a proposal that DPAs with an already adopted template will easily ignore. A unified template will have a positive impact only if it is (almost) universally adopted. In fact, there is very little contextual information about this form, there is little support information for the interpretation of the different fields and no help file for the Data Controllers, and this may end up in different implementations and interpretations. A more complete and structured description of the different fields, and a help file, would ensure a uniform interpretation and implementation.
Some more detailed comments on specific fields follow.

Section 2.1
15 It should be clearly stated that these are the high-level categories of the NACE classification, so that Data Controllers can refer to their relevant NACE codes, which can be more than one.

Section 2.2
25 National identification number: this field is not clearly described. There can be different identification numbers, and some countries could have none, so a clearer description (e.g. type of ID number, ID number) should be provided, ensuring that no ambiguity exists at least among EU countries (in some countries, more than one ID number could exist)
26 Accuracy & Responsibility: it is not clear what the checkbox is intended to confirm; if it's about taking responsibility for the accuracy of the information provided, then a standard sentence should be provided with the template, so that it is the same, as much as possible, for all DPAs. However, there is no statement about what happens if the checkbox is not checked, e.g. if the person only provides the information that someone else has prepared. Also, for 25 and 26, it is not clear when it should be applicable.

Section 2.3.1
29 It should be a Yes/No field. Also, this whole section should refer to the contact point, as described in the title, which may be the DPO if the answer to 29 is "yes". Also, "only if DPO not provided as reporting person in 1, yet" seems to be incorrect, since the reporting person is in section 2.2

Section 2.4
39,40,41 All these fields should be "For each party" and "allow multiple" (there should be multiple blocks of 39,40,41, and not multiple answers for each field)

Section 3

It could be useful to collect some information about the (un)likelihood of an impact that caused the Data Controller to notify the data breach

Section 3.1
47 What exactly is the ending date and time of the data breach, when e.g. some ransomware exfiltrated the personal data and public disclosure is being threatened, or a laptop was lost?
49 This field suggests that late notification occurs only after 72 hours, while “undue delay” can also happen with earlier notification (e.g. if the information is public)

Section 3.2
55 Should be “allow multiple”
56 It is not clear what type of loss of confidentiality is possible when personal data is not exfiltrated nor disclosed to anyone (c)
57 "Protective measures had been taken, and it is unlikely that they could be subverted" or something similar should also be included
59 It is not clear why availability, and especially temporary availability, is assessed, given that the GDPR definition of personal data violation doesn’t include availability, besides destruction which can also be complete loss of integrity. There is a practice to consider availability as data breach, but if this is the position of the EDPB, then it should be clarified, also maybe correcting the definition in art. 4 of GDPR.
60 An incident classification should map as much as possible on existing Europe-wide or international incident taxonomies, so that Data Controllers, which may need to report the same incident to different authorities, also in different countries (even if a coordination among GDPR and NIS2 notifications were achieved) can refer to a common classification, e.g. the ENISA “Reference Incident Classification Taxonomy”

Section 3.3
65 This field focuses on data subjects; however, not just the data subjects could be impacted; other natural persons could be impacted, e.g. their family members (see the Ashley Madison incident) and their rights may be relevant, as per art. 82.1 of GDPR; this would be coherent with section 4.2, where the evaluation actually refers to natural persons; in any case, it should be “allow multiple”; the same for 67 and 68 that should be grouped in blocks accordingly

Section 3.4
70 should be “allow multiple”; the same for 71, 72 and 73 that should be grouped in blocks accordingly

Section 3.5
75 Again, a taxonomy is defined (maybe derived from one adopted by a national DPA), while several taxonomies already exist (e.g. in ISO/IEC 27001/27701 or ISO/IEC 29151), tthat would better fit current practices and the assessment processes used by Data Controllers
76 This is a description of the measures; if some information about how these measures could have been subverted is required, it should be more clearly stated; however, this information probably fits better in section 3.2;

Section 4.1
87 Some clear indication on how to assess the severity should be provided; this would be one of the most beneficial impacts of a common reporting framework, ensuring assessments to be comparable among different Data Controllers and Member States, and actually helping Data Controllers in one of the most difficult and subjective evaluations.

Section 4.4
94 See section 3.5 line 75

Section 6.1

109/110 Why is this information not mandatory, considering that a coordination among authorities/control bodies would be beneficial in general, and probably mandated at some point by e.g. Digital Omnibus or similar regulation? And, how can a Data Controller state that this information is unknown, without further explanation?

Section 6.2

118 List of EEA supervisory authorit**ies.**

Section 6.3
The whole section seems to focus on data controllers outside the EEA. However, the processing by data processors outside the EEA is also relevant and should be collected, with one field block for each data processor, including the number of affected data subjects (or natural persons) etc.