Overview comments on draft **Template [2026] for personal data breach notification, Version 1.0, Adopted on 08 June 2026**

Submitted on behalf of the DPO's of the Federation of joint University Medical Centers the Netherlands (UMC NL formerly NFU).

Date: August 5, 2026

Section/ question number	***Comment***	***proposal***
General	The form seems quite extensive, and many questions are mandatory even when the question is not fitting the data breach incident in question.	The final format should include possibility to answer, "not applicable", or the form should only provide these questions when the previous answer makes those questions relevant. Even more than already provided for in the current version
General	The possibility to enter multiple of the same data breach incidents in the same form, is not available. This option is currently used in the Netherlands e.g. by health care and financial institutions	Please add the possibility of notification of multiple data breach notification in one notification submission, as now is possible in the Netherlands.
Q. 17	We understand that this is supposed to be health care related services. This contains a lot of different activities.	Please make subsections, or create the possibility of subsections (rationale) There is a difference in a pharmacy, academic hospital or mental health care
Section 2.2/2.3	This question seems mandatory to fill out; however, it creates additional workload if the person to be contacted is also the reporting person, which is very likely the case.	This could be streamlined by having a (mandatory) question by asking if the reporting person is the same as the contact person. If not, then the other details must be filled out. Or to just ask for one person's contact details. .
Q. 60	The list of incident types does not adequately reflect healthcare-specific incidents. Hospitals and university medical centers frequently report incidents involving: • unauthorised access to electronic health records (EHRs); • access without a treatment relationship; • patient record mix-ups;	Please add dedicated healthcare incident categories. (Rationale) Healthcare providers process large volumes of special category health data. The proposed categories are necessary to enable meaningful and comparable reporting across the healthcare sector.

	• patient portal incidents; • healthcare information exchange incidents.	
Q.63	The level of technical detail requested is disproportionate for an initial notification under Article 33 GDPR. .	Please limit initial notifications to high-level system descriptions and request detailed infrastructure information only in follow-up notifications. (Rationale) Large healthcare organisations often operate hundreds of interconnected clinical, administrative and research systems. Detailed forensic information is rarely available within 72 hours.
Q.68	The template assumes that organisations can determine affected individuals shortly after incident discovery. .	Please allow reporting based on affected systems or patient populations when exact numbers are unavailable. (Rationale) For cyber incidents affecting hospital systems, the number of affected patients is frequently unknown during the initial reporting period and may only become available after extensive investigation.
Q.73	The concept of "personal data records" is difficult to apply in healthcare environments.	Replace this field with: Estimated scope of affected datasets and patient records. (Rationale) A single patient file may contain thousands of medical records, laboratory results, images and documents. Counting records does not provide a meaningful indicator of risk and creates a substantial administrative burden
Q. 85	The template does not sufficiently recognise healthcare-specific consequences.	Please add: • breach of medical confidentiality; • impact on patient-provider trust; • impact on continuity of care. (Rationale)

		For healthcare organisations, breach of medical confidentiality is often the most significant consequence of a data breach and should be explicitly recognised in the template
Q. 90	Requiring a detailed description of the methodology for every notification creates unnecessary administrative burden.	Please introduce selectable options such as: • EDPB methodology; • national methodology; • healthcare sector methodology; • organisation-specific methodology. (Rationale) Hospitals already use established risk assessment methodologies and should not be required to repeatedly explain these methodologies in every notification.
Q. 106	This section requires a document to be attached. This is currently a non-mandatory field. It is possible to inform the data-subject through telephone call or in person, which is often the case in health care where a breach can only concern one patient, and it puts extra workload on health care personnel if written notification is mandatory, also in the case when the risk is not very high. Also, there is a risk that the notification contains personal data, unless redacted.	Please make the uploading of the document non-mandatory