COMPLETE SUBMISSION TO EDPB PUBLIC CONSULTATION

Template for Personal Data Breach Notification — Version 1.0, adopted on 8 June 2026

ENGLISH VERSION — READY FOR SUBMISSION

SUBMITTER INFORMATION

Field	Value
Name	María Isabel Egaña Bacarreza
Organization	QTMD (Quantum Trusted Managed Data)
Country	Chile
Email	miegana@hotmail.com
Phone	+56 9 71895745
Submitter type	Technology provider / Independent consultant
Interest in this consultation	Provide technical perspective on automated credit scoring systems and algorithmic fairness
Date	11 June 2026

TECHNICAL COMMENTS ON THE DATA BREACH NOTIFICATION TEMPLATE

---

1. Acknowledgment of the progress

I wish to commend the EDPB for adopting this common template for data breach notification (version 1.0, 8 June 2026). Standardizing notification formats is a significant step forward for harmonizing compliance with **Article 33 of the GDPR** (notification of a personal data breach to the supervisory authority) and **Article 34** (communication of a personal data breach to the data subject).

The template is comprehensive, clear, and adequately covers traditional security incidents: unauthorized access, device loss, misdelivery, malware attacks, etc. The distinction between confidentiality, integrity, and availability breaches is technically correct and useful.

Given the recent adoption of this template (8 June 2026) and the imminent full application of the EU AI Act, I believe it is critical to address the identified gap before the template becomes widely adopted by supervisory authorities across the EU.

---

2. Identification of an emerging regulatory gap

However, in the current context of the implementation of the **EU AI Act** and the growing adoption of automated decision-making systems (such as credit scoring, risk assessment, recruitment algorithms, etc.), the template presents a **significant conceptual gap**.

Identified problem: The template is designed for **discrete, detectable incidents** (a hack, a leak, a misdelivery). It does not adequately address **systemic, persistent incidents** that can occur in automated AI systems, specifically:

a) Algorithmic fairness drift – A scoring model that begins to systematically discriminate against a demographic group (e.g., gender, age, ethnic origin) after retraining or due to changes in input data. This constitutes a violation of **Article 22 of the GDPR** (automated individual decision-making) and the principles of **non-discrimination** and **accuracy**.

b) Silent performance degradation – A model whose predictions lose accuracy or calibration without the operator detecting it, affecting the accuracy of personal data processed (violation of **Article 5.1(d)** of the GDPR).

c) Undetectable manipulation of historical records – The template assumes that audit logs are intact but does not require cryptographic mechanisms to guarantee their immutability. An attacker with database access could modify historical consent or decision records without leaving a detectable trace under the current template methodology.

This gap is not limited to the EU. Chile's Financial Market Commission (CMF) is currently implementing a similar consent management system for Open Finance, and the same technical challenges have been identified in the public consultation process, confirming this is a global regulatory challenge.

3. Concrete technical proposal

I propose that the EDPB consider, in future revisions of the template or in complementary guidelines, the inclusion of a **specific category for "High-Risk Automated Decision-Making System Operational Incidents"** that includes:

3.1 New incident types

Add the following options to **Field 60 ("Nature of the incident")** in Section 3.2 ("Nature, circumstances and summary of the personal data breach"), which is currently limited to options such as "hacking", "phishing", "device lost", etc.:

- **Algorithmic fairness breach** – When an automated system begins to produce significantly biased results for a protected group, measured by standard metrics such as DPD (Demographic Parity Difference) or EOD (Equal Opportunity Difference) exceeding a threshold (e.g., > 0.05).
- **Model performance degradation** – Silent degradation of model accuracy or calibration affecting the accuracy of personal data.
- **Consent integrity breach** – Undetectable manipulation of consent or audit records due to absence of cryptographic mechanisms.

Additionally, consider adding a new option to **Field 55 ("Nature of the personal data breach")** to capture "Systemic algorithmic harm" as a distinct category alongside confidentiality, integrity, and availability breaches.

3.2 New mandatory fields for AI systems

Add the following fields to the template, mandatory when the incident involves an automated decision-making system (within the meaning of Article 22 of the GDPR). These could be implemented as a new subsection under **Section 3.2** or as conditional fields that appear when **Field 60** indicates an algorithmic incident:

Field	Description	Legal basis
Model version	Version of the AI model involved	Traceability
Fairness metrics at time of incident	DPD, EOD or other relevant fairness metrics values	Art. 22 (non-discrimination)
Consent reference	Unique identifier of the consent that enabled the processing	Art. 7 (evidence of consent)

Field	Description	Legal basis
Audit hash chain (prev_hash)	SHA-256 hash of the previous audit record, ensuring immutability	Art. 5.1(f) (integrity and confidentiality)
Automatic mitigation measures triggered	Indicate whether the system automatically suspended processing or activated corrective measures	Art. 32 (security of processing)

3.3 New recommended section

A new section **4.5 "Specific information for automated decision-making systems"** should be added (similar in structure to sections 6.2 and 6.3 for cross-border cases). This section would be conditionally displayed when the incident involves automated decision-making, similar to how **Fields 113-119** are displayed only for cross-border cases. The section should include:

- **Does the breach involve an automated decision-making system (Article 22 GDPR)?** (Yes/No/Unknown)
- **If yes, was the system subject to a Data Protection Impact Assessment (DPIA) under Article 35?** (Yes/No/Unknown - with reference)
- **Did the system have a technical fairness control loop (e.g., automatic suspension on DPD/EOD threshold exceedance)?** (Yes/No/Unknown)
- **Were fairness metrics monitored in real time?** (Yes/No/Unknown)
- **Provide hash chain of relevant audit records for independent verification** (mandatory for high-risk systems)

3.4 Enhancement to risk assessment fields

Consider adding to **Field 89 ("Outcome of the risk assessment")** a new option:

- **Systemic algorithmic harm** – When the breach affects a protected group disproportionately due to algorithmic bias, even if individual data exposure is limited.

---

4. Practical illustration: credit scoring system

As a concrete example, the **QTMD (Quantum Trusted Managed Data)** system, designed for credit scoring in Open Finance environments, implements the following mechanisms that the current template does not contemplate but are critical for data protection:

Mechanism	How it detects incidents the template misses
Immutable ledger with SHA-256 hash chaining	Any retroactive modification of consent or decision records invalidates the hash chain, immediately detectable.
Fairness control loop (DPD/EOD)	If the model begins to discriminate by gender or age (DPD/EOD ≥ 0.05), the system automatically suspends scoring and records the incident.
Cryptographic linking of decision to consent	Each credit decision contains the consent_reference. It is technically impossible for a decision to exist without a valid linked consent.
Deterministic explainability in score points	The explanation to the data subject expresses the impact of each variable in points, complying with the right to explanation under Article 22.

These elements enable **detection, reporting and mitigation** of incidents that the current template cannot adequately capture.

---

5. Benefit to the GDPR ecosystem

The inclusion of these categories and specific fields for automated systems:

1. **Raises the standard of GDPR accountability** to a cryptographically demonstrable level, not merely documentary.
2. **Aligns breach notification with the EU AI Act**, which requires continuous monitoring of high-risk systems.
3. **Reduces the burden on controllers** by standardizing how to report algorithmic drift incidents, currently in a regulatory void.
4. **Better protects data subjects** by enabling early detection of systemic discrimination, not just isolated data theft.
5. **Creates international harmonization** by addressing challenges that are emerging globally, not just in the EU.

---

6. Conclusion

The current template is an excellent starting point. However, the rapid advancement of AI and automated decision-making systems requires an evolution of the breach notification model. The most serious incidents for the rights and freedoms of data

subjects in the coming decade will likely not be credential thefts, but **undetected and unreported algorithmic biases**.

I am grateful for the opportunity to provide this technical perspective and remain at the EDPB's disposal to elaborate on any aspect of this proposal or to participate in working groups on this topic.

María Isabel Egaña Bacarreza
QTMD (Quantum Trusted Managed Data)
miegana@hotmail.com

VERSIÓN EN ESPAÑOL — LISTA PARA ENVÍO

INFORMACIÓN DEL REMITENTE

Campo	Valor
Nombre	María Isabel Egaña Bacarreza
Organización	QTMD (Quantum Trusted Managed Data)
País	Chile
Correo electrónico	miegana@hotmail.com
Teléfono	+56 9 71895745
Tipo de remitente	Proveedor tecnológico / Consultor independiente
Interés en esta consulta	Aportar perspectiva técnica sobre sistemas automatizados de scoring crediticio y equidad algorítmica
Fecha	11 de junio de 2026

COMENTARIOS TÉCNICOS AL MODELO DE NOTIFICACIÓN DE VIOLACIONES DE DATOS

---

1. Reconocimiento del avance

En primer lugar, deseo felicitar al EDPB por la adopción de este modelo común de notificación de violaciones de datos (versión 1.0, 8 de junio de 2026). La estandarización de los formatos de notificación es un avance significativo para la armonización del cumplimiento del **artículo 33 del RGPD** (notificación de violaciones de datos personales a la autoridad de control) y del **artículo 34** (comunicación de la violación al interesado).

La plantilla es completa, clara y cubre adecuadamente los incidentes de seguridad tradicionales: accesos no autorizados, pérdida de dispositivos, errores de envío, ataques de malware, etc. La distinción entre violaciones de confidencialidad, integridad y disponibilidad es técnicamente correcta y útil.

Dada la reciente adopción de esta plantilla (8 de junio de 2026) y la inminente aplicación completa del Reglamento de IA de la UE, considero crítico abordar la brecha identificada antes de que la plantilla sea ampliamente adoptada por las autoridades de control en toda la UE.

---

2. Identificación de una brecha normativa emergente

Sin embargo, en el contexto actual de implementación del **Reglamento de IA de la UE (EU AI Act)** y la creciente adopción de sistemas automatizados de toma de decisiones (como scoring crediticio, evaluación de riesgos, selección de personal, etc.), la plantilla presenta una **brecha conceptual significativa**.

Problema identificado: La plantilla está diseñada para incidentes **puntuales y detectables** (un hackeo, una filtración, un envío erróneo). Pero no contempla adecuadamente los **incidentes sistémicos y persistentes** que pueden ocurrir en sistemas automatizados de IA, específicamente:

a) Deriva de equidad algorítmica (fairness drift) – Un modelo de scoring que comienza a discriminar sistemáticamente a un grupo demográfico (ej. género, edad, origen étnico) después de un reentrenamiento o por cambio en los datos de entrada. Esto constituye una violación del **artículo 22 del RGPD** (decisiones individuales automatizadas) y de los principios de **no discriminación** y **exactitud**.

b) Degradación silenciosa del rendimiento – Un modelo cuyas predicciones pierden precisión o calibración sin que el operador lo detecte, afectando la exactitud de los datos personales tratados (violación del **artículo 5.1(d)** del RGPD).

c) Manipulación no detectable de registros históricos – La plantilla asume que los registros de auditoría son íntegros, pero no exige mecanismos criptográficos que garanticen su inmutabilidad. Un atacante con acceso a la base de datos podría modificar registros históricos de consentimiento o decisiones sin dejar rastro detectable con la metodología actual de la plantilla.

Esta brecha no se limita a la UE. La Comisión para el Mercado Financiero (CMF) de Chile está implementando actualmente un sistema similar de gestión de consentimientos para Open Finance, y los mismos desafíos técnicos han sido identificados en el proceso de consulta pública, confirmando que este es un desafío regulatorio global.

---

3. Propuesta técnica concreta

Se propone que el EDPB considere, en futuras revisiones de la plantilla o en guías complementarias, la inclusión de una **categoría específica para "Incidentes Operacionales de Sistemas Automatizados de Alto Riesgo"** que contemple:

3.1 Nuevos tipos de incidentes

Añadir al **Campo 60 ("Naturaleza del incidente")** en la Sección 3.2 ("Naturaleza, circunstancias y resumen de la violación") las siguientes opciones, actualmente limitado a opciones como "hacking", "phishing", "dispositivo perdido", etc.:

- **Violación de equidad algorítmica** – Cuando un sistema automatizado comienza a producir resultados significativamente sesgados para un grupo protegido, medido mediante métricas estándar como DPD (Demographic Parity Difference) o EOD (Equal Opportunity Difference) superiores a un umbral (ej. > 0.05).
- **Degradación del rendimiento del modelo** – Degradación silenciosa de la precisión o calibración del modelo que afecta la exactitud de los datos personales.
- **Violación de integridad del consentimiento** – Manipulación no detectable de registros de consentimiento o auditoría por ausencia de mecanismos criptográficos.

Adicionalmente, considerar añadir una nueva opción al **Campo 55 ("Naturaleza de la violación de datos personales")** para capturar "Daño algorítmico sistémico" como una categoría distinta junto a las violaciones de confidencialidad, integridad y disponibilidad.

3.2 Nuevos campos obligatorios para sistemas de IA

Añadir a la plantilla los siguientes campos, obligatorios cuando el incidente involucre un sistema automatizado de toma de decisiones (en el sentido del artículo 22 del RGPD). Estos podrían implementarse como una nueva subsección bajo la **Sección 3.2** o como campos condicionales que aparecen cuando el **Campo 60** indica un incidente algorítmico:

Campo	Descripción	Fundamento normativo
Versión del modelo	Versión del modelo de IA involucrado	Trazabilidad
Métricas de equidad en el momento del incidente	Valores de DPD, EOD u otras métricas de equidad relevantes	Art. 22 (no discriminación)
Referencia al consentimiento	Identificador único del consentimiento que habilitó el tratamiento	Art. 7 (prueba del consentimiento)
Cadena de hash de auditoría (prev_hash)	Hash SHA-256 del registro de auditoría anterior, garantizando inmutabilidad	Art. 5.1(f) (integridad y confidencialidad)
Medidas de mitigación automática activadas	Indicar si el sistema suspendió automáticamente el procesamiento o activó medidas correctivas	Art. 32 (seguridad del tratamiento)

3.3 Nueva sección recomendada

Se sugiere añadir una sección **4.5 "Información específica para sistemas automatizados de toma de decisiones"** (similar en estructura a las secciones 6.2 y 6.3 para casos transfronterizos). Esta sección se mostraría condicionalmente cuando el incidente involucre toma de decisiones automatizada, similar a cómo los **Campos 113-119** se muestran solo para casos transfronterizos. La sección debe incluir:

- **¿El incidente involucra un sistema automatizado de toma de decisiones (artículo 22 del RGPD)?** (Sí/No/No se sabe)

- **En caso afirmativo, ¿el sistema fue sometido a una Evaluación de Impacto de Protección de Datos (DPIA) según el artículo 35?** (Sí/No/No se sabe - con referencia)
- **¿El sistema contaba con un lazo de control técnico de equidad (ej. suspensión automática ante superación del umbral DPD/EOD)?** (Sí/No/No se sabe)
- **¿Se monitorizaron las métricas de equidad en tiempo real?** (Sí/No/No se sabe)
- **Proporcionar la cadena de hash de los registros de auditoría relevantes para verificación independiente** (obligatorio para sistemas de alto riesgo)

3.4 Mejora a los campos de evaluación de riesgo

Considerar añadir al **Campo 89 ("Resultado de la evaluación de riesgo")** una nueva opción:

- **Daño algorítmico sistémico** – Cuando la violación afecta desproporcionadamente a un grupo protegido debido a sesgo algorítmico, incluso si la exposición de datos individuales es limitada.

---

4. Ilustración práctica: sistema de scoring crediticio

A modo de ejemplo concreto, el sistema **QTMD (Quantum Trusted Managed Data)**, diseñado para scoring crediticio en entornos Open Finance, implementa los siguientes mecanismos que la plantilla actual no contempla pero que son críticos para la protección de datos:

Mecanismo	Cómo detecta incidentes que la plantilla omite
Ledger inmutable con encadenamiento de hash SHA-256	Cualquier modificación retroactiva de registros de consentimiento o decisiones invalida la cadena de hashes, detectable inmediatamente.
Lazo de control de equidad (DPD/EOD)	Si el modelo comienza a discriminar por género o edad (DPD/EOD ≥ 0.05), el sistema suspende automáticamente el scoring y registra el incidente.
Vinculación criptográfica de la decisión al consentimiento	Cada decisión de crédito contiene la referencia_al_consentimiento. Es técnicamente imposible que exista una decisión sin un consentimiento válido vinculado.

Mecanismo	Cómo detecta incidentes que la plantilla omite
Explicabilidad determinista en puntos de score	La explicación al interesado expresa el impacto de cada variable en puntos, cumpliendo con el derecho a obtener explicación del artículo 22.

Estos elementos permiten **detectar, reportar y mitigar** incidentes que la plantilla actual no puede capturar adecuadamente.

---

5. Beneficio para el ecosistema del RGPD

La inclusión de estas categorías y campos específicos para sistemas automatizados:

1. **Eleva el estándar de responsabilidad (accountability) del RGPD** a un nivel criptográficamente demostrable, no meramente documental.
2. **Alinea la notificación de violaciones con el EU AI Act**, que exige monitoreo continuo de sistemas de alto riesgo.
3. **Reduce la carga para los responsables del tratamiento** al estandarizar cómo reportar incidentes de deriva algorítmica, actualmente en un vacío normativo.
4. **Protege mejor a los interesados** al permitir la detección temprana de discriminación sistémica, no solo robos de datos aislados.
5. **Crea armonización internacional** al abordar desafíos que están emergiendo globalmente, no solo en la UE.

---

6. Conclusión

La plantilla actual es un excelente punto de partida. Sin embargo, el rápido avance de la IA y los sistemas automatizados de toma de decisiones exige una evolución del modelo de notificación de violaciones. Los incidentes más graves para los derechos y libertades de los interesados en la próxima década probablemente no serán robos de credenciales, sino **sesgos algorítmicos no detectados y no reportados**.

Agradezco la oportunidad de aportar esta perspectiva técnica y quedo a disposición del EDPB para ampliar cualquier aspecto de esta propuesta o participar en grupos de trabajo sobre este tema.

María Isabel Egaña Bacarreza
QTMD (Quantum Trusted Managed Data)
miegana@hotmail.com