

Obligaciones de protección de datos tras el cierre del programa

Conservación · Diplomas · Roles post-cierre · Brechas a posteriori

Dirigido a Entidades Adheridas (CGATE y Colegios Profesionales)

Delegado de Protección de Datos
De Lorenzo Abogados · Área Digital

Julio 2026



Art. 17 RGPD · Art. 8.4 RD 876/2024 · Los datos no desaparecen con el cierre — se bloquean, custodian y destruyen conforme a plazos legales

5

años mínimo de conservación
desde el fin del periodo de
justificación PRTR

Art. 8.4 RD 876/2024
Art. 132 Regl. Financiero UE



Bloquear el acceso desde el cierre operativo

Los datos del programa dejan de estar disponibles para uso operativo en cuanto se cierra el proyecto. No pueden seguir usándose para ninguna finalidad formativa ni de gestión una vez concluido. Línea 1 (SUG) aplica restricciones de acceso desde el cierre.



Custodiar de forma segura durante el plazo legal

Cada entidad conserva bajo su responsabilidad los datos que trató en su ámbito: inscripciones, asistencia, evaluaciones. Durante todo el periodo de conservación siguen siendo datos personales sujetos al RGPD — cualquier incidente sobre ellos genera las mismas obligaciones que durante el programa.



Destruir coordinadamente cuando venzan los plazos

Vencido el plazo, los datos deben borrarse o anonimizarse. Ninguna entidad lo hace unilateralmente: la destrucción se coordina con UP, la autoriza el DPD y se documenta como evidencia de cumplimiento. Ejecutar antes de plazo compromete la justificación PRTR.

El diploma tiene dos vidas jurídicas con plazos distintos — ambas obligan a conservarlo por razones que no siempre coinciden

2

finalidades que coexisten en el mismo documento

Acreditación del alumno

Sin plazo fijo — durante la vida útil del título

El participante puede necesitar acreditar que completó el programa en cualquier momento, incluso años después. UP y las EA deben poder emitir duplicados o certificar la autenticidad del diploma mientras sea razonablemente posible.

Justificación de la subvención PRTR

Mínimo 5 años desde el fin del periodo de justificación

El diploma es evidencia justificativa de que los fondos Next Generation EU se destinaron a su fin. Plazo mínimo obligatorio: 5 años desde el fin del periodo de justificación (art. 8.4 RD 876/2024 y art. 132 Reglamento Financiero UE). Accesible para auditoría de Red.es.

El DNI no es parte del diploma — tiene su propio plazo

El documento de identidad aportado para verificación de colegiación se conserva separadamente, con marca de agua y acceso restringido, sujeto al mismo plazo PRTR. No se destruye junto con el diploma ni antes de que venza ese plazo.

Regla práctica

Conservar el diploma hasta que venzan AMBOS plazos. El más largo es el que prevalece. Documentar qué entidad emitió cada diploma, en qué formato está disponible y cómo puede el alumno obtener una copia en el futuro.

Art. 5 RGPD · Art. 32 LOPDGDD · Instrucciones de gestión de conservación y exactitud

Principio de exactitud (art. 5.1.d)

Los datos deben ser exactos, actualizados y rectificados sin dilación si son inexactos. La inexactitud conocida y no corregida es ya un incumplimiento.

Principio de limitación del plazo (art. 5.1.e)

Los datos solo se conservan durante el tiempo necesario para la finalidad. Después: supresión, bloqueo o anonimización. Nunca conservación indefinida sin base jurídica.

Base jurídica para conservar más allá de la finalidad

Obligación legal · Misión interés público · Interés legítimo defensa jurídica · Control PRTR/subvenciones. Sin base → no se conserva.

Plazos clave por tipo de dato

Participantes

Inscripción	5 años
Evaluaciones	5 años
Certificados	5 años
Comunicaciones	3 años

Subvenciones / PRTR

Justificación económica	Mín. 5 años
Auditorías PRTR	5 años

Fiscal / Contable

Facturas	6 años
Tributario	4 años

Protección de datos

RAT / DPA	3 años
Ejercicio de derechos	3 años

Regla: si no hay base jurídica para conservar → no se conserva. El vencimiento del plazo no es automático — requiere proceso documentado (Anexo II).

Art. 32 LOPDGDD · Bloquear ≠ borrar · Anonimizar ≠ seudonimizar

Bloqueo de datos (art. 32 LOPDGDD) — NO es borrar

Es: identificar y reservar · impedir tratamiento activo · mantener solo para autoridades competentes.

Se aplica cuando: todavía no ha transcurrido el plazo legal para exigir responsabilidades · hay posibles reclamaciones pendientes · hay control de Red.es / PRTR.

Durante el bloqueo: sin uso ordinario · sin acceso operativo · solo disponible para autoridad competente.

Supresión definitiva — cómo hacerlo bien

Papel: destrucción física segura · empresa homologada · certificado de destrucción obligatorio.

Digital: borrado seguro · eliminación en TODOS los sistemas · registro técnico de borrado. Sin certificado → no hay evidencia de cumplimiento.

Anonimización vs. seudonimización

Anonimización

- Irreversible
- Sale del ámbito del RGPD
- No permite reidentificación
- No es una simple codificación

Seudonimización

- Existe clave separada
- Sigue siendo dato personal
- Requiere medidas reforzadas
- Riesgo de reidentificación

Roles en el proceso de conservación/destrucción

Comisión de Coordinación:

Aprueba criterios y decisiones excepcionales

DPO:

Supervisa y valida jurídicamente.
No ejecuta

Resp. de Calidad:

Trazabilidad y evidencia

Resp. de Área:

Decide propuesta concreta

Tecnología:

Ejecuta borrado, bloqueo o anonimización

El proyecto termina. Las responsabilidades sobre los datos, no — Art. 12-22 RGPD · 1 mes de plazo desde cualquier solicitud



el cierre del proyecto no extingue la
responsabilidad sobre los datos tratados

Corresponsabilidad
y encargos vigentes
hasta destrucción

Qué persiste: la responsabilidad sobre los datos

Cada entidad sigue siendo responsable de los datos que trató en su ámbito.
La corresponsabilidad con UP y los contratos de encargo art. 28 permanecen vigentes hasta que los datos sean destruidos o anonimizados conforme a los plazos legales.

Ejercicios de derechos que lleguen después del cierre

Los participantes pueden ejercer sus derechos (acceso, supresión, rectificación, oposición) incluso después del cierre. El circuito sigue siendo el mismo: Red.es recibe → coordina con UP/DPD → EA o Línea aporta la información. El plazo de 1 mes del art. 12 RGPD corre desde que CUALQUIER entidad de la cadena recibe la solicitud.

Qué NO puede hacer cada entidad sola

Ninguna EA responde directamente a solicitudes de participantes ni a requerimientos externos (Red.es, AEPD) sin notificar antes al DPD.
Ninguna EA destruye datos ni diplomas sin instrucción formal de UP. Ante la duda: contactar primero con el DPD.

Relación con Red.es durante el periodo de conservación

Red.es mantiene acceso al SUG en modo SaaS durante todo el periodo de conservación para fines de auditoría PRTR. Puede requerir información en cualquier momento. Cualquier requerimiento de Red.es dirigido a una EA debe canalizarse a través del DPD antes de dar respuesta.

Arts. 15-22 RGPD · 7 derechos con sus límites de denegación

Acceso

Saber si tratamos sus datos y obtener copia.

Se puede denegar si:

No tratamos sus datos · Afecta a derechos de terceros.

Rectificación

Corregir datos inexactos o incompletos.

Se puede denegar si:

Los datos son correctos · No pueden modificarse (ej. videovigilancia).

Supresión

Eliminar datos cuando ya no son necesarios o el tratamiento es ilícito.

Se puede denegar si:

Obligación legal de conservación · Necesarios para defensa · Interés público prevalente.

Limitación

Bloquear temporalmente el uso de datos.

Se puede denegar si:

No concurre causa legal (impugnación, oposición, ilicitud, etc.).

Portabilidad

Recibir datos en formato estructurado o transmitirlos a otro responsable.

Se puede denegar si:

Tratamiento no automatizado · No basado en consentimiento o contrato · Técnicamente imposible.

Oposición

Solicitar que dejemos de tratar datos basados en interés legítimo o público. En marketing directo → NO se puede denegar.

Se puede denegar si:

Motivos legítimos imperiosos que prevalecen · Necesario para defensa jurídica.

No decisiones automatizadas

No ser objeto de decisiones solo automatizadas con efectos jurídicos.

Se puede denegar si:

Autorizado por ley · Necesario para contrato · Consentimiento explícito.

Canal único: sede electrónica Red.es · Plazo: 1 mes desde recepción por cualquier entidad

1 Interesado

Ejerce el derecho formalmente a través de la sede electrónica de Red.es (canal obligatorio).



2 Red.es

Recibe y deriva a Línea 1 + Entidad Adherida. El reloj de 1 mes empieza aquí.



3 EA / Línea 1

Analiza, ejecuta y responde. Informa a Red.es para cierre del expediente.



4 Red.es

Cierra el expediente y comunica la resolución al interesado. Plazo máximo: 1 mes (+ 2 adicionales con aviso en el primer mes).

Si una EA recibe directamente una solicitud de derecho → NO tramitar · reconducir al canal oficial (Anexo I: comunicado de rechazo con enlace a sede Red.es) · REGISTRAR la entrada. El plazo sigue corriendo.

Registro obligatorio

- Fecha de entrada
- Derecho ejercido
- Identificación del solicitante
- Plazo máximo de respuesta
- Trazabilidad siempre

Plazos

- 1 mes desde recepción
- Ampliación: hasta 2 meses adicionales (avisar en el primer mes)
- Denegación: motivada + informar derecho a reclamar ante AEPD

Verificación de identidad

- Solo si hay dudas razonables
- No se solicita DNI automáticamente
- Proporcionalidad: no hacer difícil el ejercicio del derecho

LSSI — comunicaciones electrónicas: prohibido enviar emails promocionales sin consentimiento previo expreso (opt-in). Excepción: relación contractual previa + servicios similares + mecanismo de baja en cada email. Usar Anexo II (modelo de baja comercial) para separar circuito LSSI del circuito RGPD.

Art. 33 RGPD · Un incidente detectado después del cierre genera exactamente las mismas obligaciones que si el programa siguiera activo

72h

plazo máximo para notificar a la AEPD desde que se tiene conocimiento

*No desde que se confirma.
No desde que se evalúa.
Desde que se sabe.*

1 Detectar y comunicar el mismo día

Cualquier acceso no autorizado, pérdida, alteración o destrucción de datos del programa — aunque el proyecto esté cerrado — se comunica al DPD y a UP el mismo día. No esperar a confirmar la gravedad. La sospecha ya activa el protocolo.

2 Evaluar el riesgo con el DPD

El DPD determina: ¿riesgo real para los derechos del participante? Si es alto → notificación a la AEPD (72 h, art. 33) y comunicación a los afectados (art. 34). Esa decisión no la toma cada entidad por separado — siempre con el DPD.

3 Registrar siempre, independientemente de la gravedad

Todo incidente queda registrado en el inventario del DPD (art. 33.5 RGPD), aunque no se notifique a la AEPD. El registro es obligatorio con independencia del nivel de riesgo y de si el programa está cerrado. No hay excepciones.

4 Identificar quién custodia los datos afectados

La responsabilidad recae en la entidad que custodia los datos en el momento del incidente. Por eso es crítico saber exactamente qué datos quedan bajo custodia de cada EA y en qué sistemas — esa documentación es la base para gestionar cualquier brecha post-cierre.

Para llevarse de esta reunión

Tres reglas para las Entidades Adheridas a partir de ahora

De Lorenzo
A B O G A D O S

1

Los datos no desaparecen con el cierre

Cada entidad sigue siendo responsable de los que trató, hasta que sean destruidos conforme a los plazos legales. La correspondencia y los encargos siguen vigentes. Ninguna destrucción se hace sola: se coordina, se autoriza por el DPD y se documenta.

2

Los plazos legales no esperan al cierre del proyecto

Una solicitud de derechos recibida mañana genera el mismo plazo de 1 mes que durante el programa. Una brecha detectada en seis meses genera el mismo plazo de 72 h. El cierre del proyecto no congela los relojes del RGPD.

3

Primero el DPD, después la respuesta

Ante cualquier incidente, solicitud de derechos o requerimiento de Red.es o la AEPD: contactar primero con el DPD antes de dar respuesta. dpo@delorenzoabogados.es · El encargo DPD cubre el periodo de conservación.