E-learning y RGPD: claves para una formación online segura y conforme a la normativa

Dirigido a responsables de RRHH, Formación, Compliance e IT de PYMEs que utilizan o están valorando implantar un LMS

e·xplicate

www.e-xplicate.com

Índice de contenidos

¿Por qué el RGPD afecta a tu plataforma de formación?

Cuando una empresa implanta un sistema de gestión del aprendizaje (LMS), habitualmente se pone el foco en los contenidos, la experiencia de usuario o el coste de la solución. Sin embargo, hay una dimensión que con frecuencia queda en segundo plano: el **tratamiento de datos personales** que conlleva cualquier plataforma de formación online.

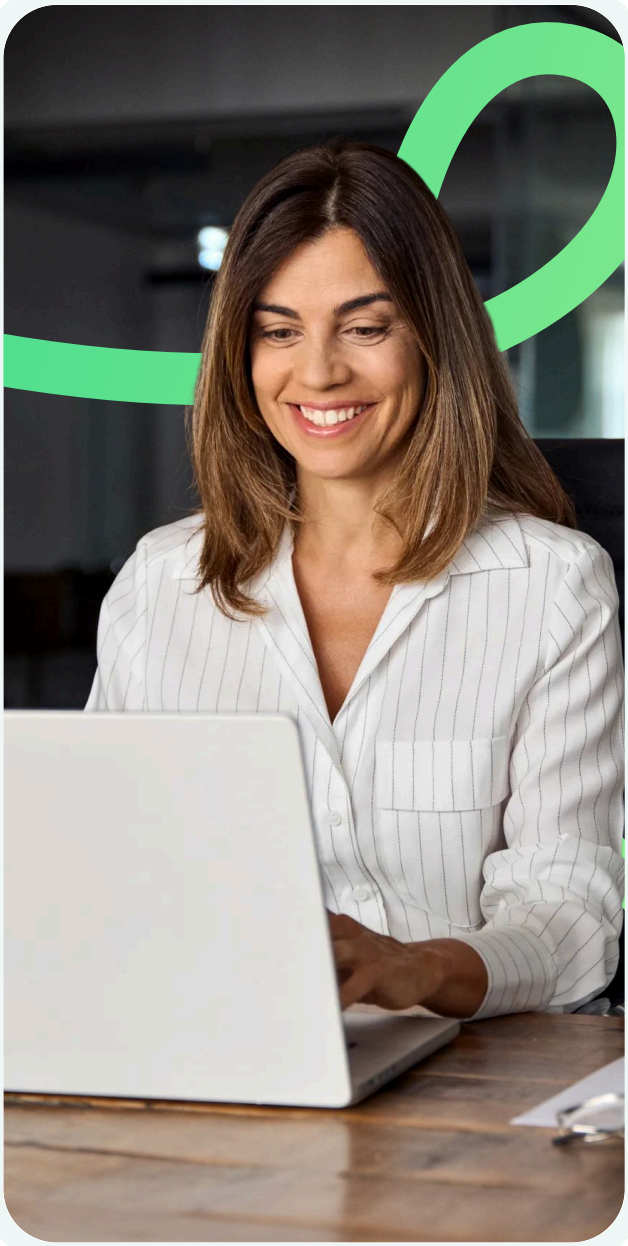
Un **LMS recoge, almacena y procesa datos** de los empleados de forma continua: nombres, correos corporativos, resultados de evaluaciones, tiempo dedicado a cada módulo, fechas de acceso, historial de intentos... Todos estos datos son datos personales según el Reglamento General de Protección de Datos (RGPD, Reglamento UE 2016/679) y su tratamiento debe estar debidamente legitimado, documentado y protegido.

El incumplimiento puede derivar en **sanciones económicas relevantes** (de hasta 20 millones de euros o el **4% de la facturación global anual**), pero también en pérdida de confianza por parte de los empleados y daño reputacional. Para una PYME, las consecuencias de una brecha de seguridad o una reclamación ante la Agencia Española de Protección de Datos (AEPD) pueden ser especialmente sensibles.

La buena noticia es que cumplir con el RGPD en el ámbito del e-learning corporativo no es un proceso inabarcable. Requiere planificación, pero es perfectamente alcanzable con las herramientas y el enfoque adecuados.

Qué datos trata un LMS y bajo qué base legal

Tipos de datos habituales en un LMS corporativo



1. Datos identificativos: nombre, apellidos, correo electrónico, número de empleado.

2. Datos de seguimiento y desempeño: progresos por curso, puntuaciones, tiempos de conexión, intentos de evaluación.

3. Datos técnicos: dirección IP, dispositivo utilizado, logs de acceso.

4. Datos de asignación formativa: cursos obligatorios, itinerarios asignados, estado de certificación.

Bases jurídicas aplicables:

En el contexto de la formación corporativa, las bases jurídicas más frecuentemente invocadas son dos:

- ✓ Ejecución de un contrato o relación laboral (art. 6.1.b RGPD): cuando la formación es obligatoria para el desempeño del puesto o está vinculada a las condiciones laborales.

- ✓ Interés legítimo del responsable del tratamiento (art. 6.1.f RGPD): cuando la empresa tiene un interés real y documentado en la gestión del conocimiento y el desarrollo del empleado.

Es importante que la base legal esté clara antes de poner en marcha la plataforma, ya que condiciona los derechos que pueden ejercer los interesados y cómo se debe documentar el tratamiento en el Registro de Actividades de Tratamiento (RAT).

Nota práctica:

La formación relacionada con el cumplimiento normativo (prevención de riesgos, protección de datos, igualdad...) tiene una base legal especialmente sólida al estar respaldada por obligaciones legales específicas (art. 6.1.c RGPD).

Documenta siempre qué normativa respalda cada programa formativo obligatorio.

Los 5 puntos clave de cumplimiento que debes revisar

A continuación, se recogen los aspectos que con mayor frecuencia presentan deficiencias en entornos de e-learning corporativo y que suelen ser objeto de atención por parte de la AEPD:

3.1. Contrato de encargo de tratamiento con el proveedor del LMS

Si la plataforma de formación está alojada o gestionada por un tercero (proveedor SaaS, empresa de desarrollo, consultora...), ese proveedor actúa como encargado del tratamiento. El RGPD exige que la relación quede formalizada mediante un contrato específico que recoja, entre otros aspectos, las instrucciones de tratamiento, las medidas de seguridad aplicadas, los subencargos autorizados y los protocolos ante brechas de seguridad.

Verificar que este contrato existe y está actualizado es uno de los primeros pasos a dar.

3.2. Información transparente a los empleados

Los empleados tienen derecho a saber que sus datos serán tratados en la plataforma de formación, con qué finalidad, durante cuánto tiempo y qué derechos pueden ejercer. Esta información debe facilitarse de forma clara y accesible, habitualmente en el momento de la incorporación a la empresa o antes del primer acceso al LMS.

Una práctica habitual es incluir una cláusula específica en el contrato de trabajo o en el manual del empleado, así como mostrar una pantalla informativa en el primer inicio de sesión en la plataforma.

3.3. Plazos de conservación de los datos

¿Cuánto tiempo se conservan los registros de formación de un empleado que ya ha causado baja? ¿Se bloquean o se eliminan de forma automática?

La ausencia de una política de retención definida es una de las brechas más comunes.

3.4. Control de accesos y seguridad técnica

No todos los usuarios de la organización deben tener acceso a todos los datos. Un tutor solo necesita ver el progreso del alumno; el departamento de RRHH puede requerir datos de certificación, pero no los registros de navegación. La gestión de accesos por roles es una obligación derivada del principio de minimización, y debe estar documentada y revisada periódicamente.

Desde el punto de vista técnico, el LMS debe contar con cifrado de datos en tránsito y en reposo (certificado SSL/HTTPS), copias de seguridad periódicas y un sistema de alertas ante incidentes de seguridad.

3.5. Registro de Actividades de Tratamiento (RAT)

El uso de un LMS debe quedar reflejado en el RAT de la organización, con independencia de si la empresa está obligada formalmente a mantenerlo. Este registro debe recoger la finalidad del tratamiento, las categorías de datos y de interesados, los plazos de conservación, las medidas de seguridad y, en su caso, las transferencias internacionales.

Mantenerlo actualizado es la base de cualquier auditoría o reclamación ante la AEPD.

Buenas prácticas para una formación online conforme al RGPD

El cumplimiento no se logra con un único documento legal: requiere decisiones técnicas, organizativas y culturales que se refuercen mutuamente.

A continuación se recogen las principales buenas prácticas, agrupadas por ámbito.

A Minimización y gestión ética de los datos

La regla de oro es: «Si no lo necesitas, no lo pidas». La minimización de datos implica solicitar únicamente la información estrictamente necesaria para la prestación del servicio formativo. Esto se traduce en evitar almacenar datos especialmente sensibles —opiniones políticas, datos de salud, información biométrica— salvo que exista una obligación legal expresa que lo justifique.

Cuando se usen plataformas con formularios de registro propios, hay que asegurarse de que el consentimiento sea libre, específico, informado e inequívoco. Olvida las casillas pre-marcadas: el usuario debe hacer clic activamente antes de que su información sea procesada.

B Privacidad desde el diseño (Privacy by Design)

El RGPD impulsa el enfoque de «Privacy by Design», que consiste en incorporar la privacidad desde la concepción de cualquier curso o plataforma, no como un añadido posterior.

En la práctica, esto implica:

- ☑ Diseñar formularios que solo recojan datos esenciales.
- ☑ Configurar el LMS para limitar la visibilidad de la información según el rol de cada usuario.
- ☑ Aplicar técnicas de anonimización o pseudonimización cuando se analicen estadísticas o resultados agregados.
- ☑ Establecer plazos de retención y automatizar la eliminación de datos que ya no sean necesarios.
- ☑ Incluir alertas de seguridad y notificaciones automáticas en caso de incidentes.

C Infraestructura técnica robusta

El LMS es el repositorio donde se almacena información sensible sobre los empleados. La elección del proveedor y la configuración técnica de la plataforma tienen un impacto directo en el nivel de cumplimiento. Además de los certificados SSL y el cifrado mencionados en el punto 3.4, es recomendable realizar auditorías técnicas periódicas para verificar que las medidas de seguridad se mantienen actualizadas y son proporcionales al riesgo.

A la hora de elegir proveedor, conviene verificar que cuente con certificaciones reconocidas que acrediten su nivel de seguridad. Algunos indicadores clave que hay que solicitar y contrastar:

- ✓ Certificación ISO 27001: garantiza que el proveedor gestiona la seguridad de la información mediante un sistema auditado y homologado internacionalmente.
- ✓ Centros de datos TIER 3: aseguran una disponibilidad del 99,982% y redundancia en los sistemas críticos, lo que reduce el riesgo de pérdida de datos o interrupción del servicio.
- ✓ Cumplimiento de OWASP: indica que el desarrollo de la plataforma sigue las mejores prácticas para prevenir las vulnerabilidades de seguridad más habituales en aplicaciones web.

Pedir estas acreditaciones documentadas antes de firmar un contrato con un proveedor de LMS es una práctica recomendable y coherente con el principio de responsabilidad proactiva que exige el RGPD.

En e-xplicate ofrecemos máxima seguridad y cumplimos con los más altos estándares: OWASP, centros de datos TIER 3 y certificación de seguridad ISO 27001.

D Transparencia y cultura de privacidad

La transparencia no consiste en tener un documento legal escondido en el pie de página. Implica informar de forma clara y accesible sobre quién es el responsable de los datos, para qué se usan y cuánto tiempo se van a conservar, y hacerlo en el momento en que los empleados acceden por primera vez a la plataforma.

El factor humano es determinante: la mayoría de las brechas de seguridad se deben a errores humanos (contraseñas compartidas, correos enviados a destinatarios erróneos, descargas de datos sin autorización). Formar al equipo en buenas prácticas de protección de datos es tan importante como contar con la mejor infraestructura técnica.

El papel del DPO y la coordinación interna

En función del volumen y la naturaleza de los tratamientos, algunas organizaciones están obligadas a contar con un Delegado de Protección de Datos (DPO).
Aunque para muchas PYMEs este rol no es obligatorio, sí es recomendable designar internamente a una persona responsable de supervisar el cumplimiento en materia de protección de datos relacionado con la formación online.

Esta figura debe actuar como punto de contacto entre el departamento de RRHH o Formación, el área de IT y el proveedor del LMS.
La coordinación entre estas áreas es clave para evitar que las decisiones técnicas —actualizaciones del sistema, cambios de proveedor, integración con otros sistemas de RRHH— generen nuevos riesgos de cumplimiento sin que el área responsable de privacidad tenga conocimiento.

Es igualmente recomendable realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) cuando se implanta un nuevo LMS o se incorporan funcionalidades que implican un tratamiento a gran escala o de datos especialmente sensibles, como pueden ser evaluaciones psicométricas o datos de salud en formaciones de prevención de riesgos.

Conclusión

Garantizar la **seguridad y legalidad en el e-learning** no es solo una obligación legal, sino también una ventaja competitiva. Las organizaciones que protegen los datos de sus usuarios:

- Generan mayor confianza
- Evitan sanciones y riesgos legales
- Mejoran la reputación y la experiencia del alumno

Cumplir con el RGPD es un proceso continuo que combina **tecnología, formación y buenas prácticas**, adaptándose a cada tipo de plataforma y público.

Si buscas un LMS en línea con los más altos estándares de seguridad, en e-xplicate o tenemos.

Contáctanos y solicita una demo gratuita.

Recursos de referencia

Para profundizar en los aspectos tratados en esta guía, se recomiendan los siguientes recursos oficiales:

- Agencia Española de Protección de Datos (AEPD): www.aepd.es — guías sectoriales, resoluciones y recursos formativos gratuitos.
- Comité Europeo de Protección de Datos (CEPD): edpb.europa.eu — directrices europeas sobre bases jurídicas, transferencias internacionales y EIPD.
- Portal de transparencia del RGPD de la Comisión Europea: disponible en eur-lex.europa.eu.
- Guía de privacidad en el ámbito laboral de la AEPD: documento específico sobre el tratamiento de datos de empleados, disponible en el portal de la AEPD.