SITPRE

Programa de
Ingeniería de Sistemas
Acreditado de Alta Calidad
"Educación y Tecnología con Compromiso Social"

La Ley de protección de datos en los colegios y centros educativos no se circunscribe a una simple normativa. Afecta a varios aspectos muy distintos y a los sistemas de información del colegio, lo que quiere decir que es una cuestión bastante más medular de lo que puede parecer.

Ley de Protección de datos de carácter personal (LOPD) fue aprobada en 1999 y la Agencia de protección de Datos (AEPD) es la autoridad estatal de control independiente, encargada de velar por el cumplimiento de la normativa, garantizando y tutelando el derecho fundamental a la protección de datos de carácter personal de los ciudadanos. Es importante saber que las imágenes se consideran datos protegidos en tanto en cuanto sirven para identificar a una persona física.

Los datos de carácter personal se dividen en tres categorías con sus correspondientes niveles de seguridad:

A: Datos personales básicos y generales, les corresponde un nivel de seguridad Básico

B: Datos personales de infracciones, agencia tributaria de morosidad, bancarios, seguridad social, personalidad, que les corresponde un Nivel de seguridad media

C: Datos de ideología, religión, afiliación sindical, vida sexual, policiales o violencia de género que les corresponde un Nivel de seguridad máximo

En este marco, las principales obligaciones que tienen que tener en cuenta un colegio para el cumplimiento de la Ley son las siguientes:

1.-La primera obligación será el registro del uno o varios ficheros en la Agencia de protección de datos. Como mínimo fichero de datos personales de alumnos, padres y personal del centro. Eso se puede hacer online a través de este formulario en la propia Agencia de Protección de Datos: https://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/servicioNOTA.jsf

2.- En el proceso de matriculación, donde se recaban los datos, es fundamental informar a los padres del uso y existencia de esos ficheros y que estos den su autorización para los usos que se vayan a realizar (web del colegio, cesión a terceros para determinados usos,..etc.)

3.-Los ficheros de datos de menores de edad deben de contar con el consentimiento de progenitores o tutores legales sin que reciban un tratamiento especial por ser menores. Los datos académicos corresponden a un nivel de seguridad medio. Los mayores de 14 años pueden prestar ellos mismos el consentimiento para cierto tipo de datos. Por supuesto hay que otorgar de forma efectiva los derechos de acceso, rectificación u oposición de las personas físicas que soliciten este derecho.

4.- El régimen sancionador es fuerte, con lo que es muy importante para el colegio no incurrir en una infracción. Además la imagen del centro o de las personas puede tener graves perjuicios. Por tener unas cifras y saber de qué estamos hablando estas son las principales sanciones

Leves: entre 600 y 60.000€ aprox. Corresponden a no solicitar la inscripción del fichero, recopilar datos sin informar previamente, no atender a los derechos de rectificación o cancelación ni a los requerimientos de la Agencia de Protección de datos

Graves: de 60.000 a 300.000 aprox. Corresponden a no inscribir el fichero, no tener consentimiento para recabar datos, utilizarlos para otra función, no permitir acceso, rectificación, no seguir las garantías de la AEPD, mantener ficheros sin garantía de seguridad

Muy graves: de 300.000 a 600.000. Crear ficheros de datos especialmente protegidos, recogida de datos engañosa, comunicación de datos, tratamiento ilegitimo, transferencia de datos a países que no cumplen normativa o no atender sistemáticamente los requerimientos de la AEPD

La custodia de los datos, a través de unas adecuadas medidas de seguridad, resulta fundamental ya que una filtración de datos podría originar actuaciones de oficio contra el centro como ha ocurrido en alguna ocasión.

5- Todo colegio o centro educativo tiene que tener redactado el Documento de Seguridad.

Este es un documento interno que recoge todas las normas, procedimientos de seguridad, medidas y reglas encaminadas a garantizar la seguridad de los datos y debe de estar elaborado por el responsable del fichero y encargado del tratamiento de los datos. Igualmente debe de informarse a todo el personal y es de obligado cumplimiento por este. Como mínimo debe de comprender detalles de recursos protegidos, medidos de seguridad, normas y procedimientos, funcionales y obligaciones del personal, estructura de los ficheros, procedimientos de notificación y gestión ante incidencias

Para los niveles medios y altos se exige además un responsable de seguridad y medidas para revisión periódica.

Aquí se puede ver una guía de documento de seguridad:

https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php

Entre los aspectos más importantes del documento de seguridad, esta que la validación de usuarios debe de ser personal e inequívoca, debe de existir un registro de acceso y cada usuario solo debe de acceder a los datos que son necesarios para el desempeño de su puesto. Estas son características que vienen dadas por el programa o plataforma de gestión del colegio.

6.- Medidas de seguridad adecuadas y ubicación de los datos: El documento de seguridad lleva implícito una serie de medidas de seguridad. En el caso de que los datos se hallen en la Nube el colegio tendrá que asegurarse que los datos se hallan en España o en la Unión Europea (y no bastara que el fabricante del software este en España o un Pais de legislación perecida, es decir, Unión Europea. Algunas plataformas pueden usar Google u Amazon que normalmente no garantizan que sus datos estén en la Unión Europea.

Es importante considerar que una plataforma online simplifica mucho el cumplimiento de la Ley de Protección de datos, ya que incluye las medidas de seguridad, tratamiento de copias, acceso jerarquizado, registro de acceso. Resulta fundamental en estos casos que incluya protocolo seguro lo que significa que la información está cifrada. En este sentido la AEPD da su respaldo a Microsoft, reconociendo la solvencia y las garantías de los servicios corporativos de Microsoft en la Nube en lo relativo a transferencias internacionales de datos. Igualmente la AEPD afirma que los contratos de Microsoft ofrecen garantías adecuadas para que los clientes confíen sus datos personales a la compañía en el marco de los servicios corporativos de Office 365, Dynamics CRM Online y Microsoft Azure. Microsoft es el primer y único proveedor que recibe este reconocimiento de la Agencia de Protección de Datos:
http://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/auto_transf_2014/common/pdfs/TI-00032-2014_Resolucion-de-fecha-09-05-2014_de-MICROSOFT-CORPORATION_a-Estados-Unidos.pdf

https://news.microsoft.com/es-es/2014/06/06/aepd-servicios-cloud-microsoft/#sm.00110oxtl17i4d6zsqd13of55csw7

7.- Los sistemas de vídeo vigilancia no deben de grabar fuera del recinto del colegio y estar debidamente identificadas las cámaras. También tienes que estar identificados e informados los sistemas de control laboral o control de acceso general al centro o a determinados recintos (como comedor) a través de huella digital.