Comunidad de Madrid

Delegación de Protección de Datos
CONSEJERÍA DE EDUCACIÓN,
UNIVERSIDADES, CIENCIA Y PORTAVOCÍA

INSTRUCCIONES SOBRE PROTECCIÓN DE DATOS PERSONALES PARA LOS CENTROS EDUCATIVOS PÚBLICOS DE LA COMUNIDAD DE MADRID

Versión 2.0

El marco normativo esencial en lo referente al derecho a la privacidad lo constituyen el Reglamento General Europeo de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que adapta la legislación española al Reglamento General de Protección de Datos de la Unión Europea.

A continuación, presentamos unas instrucciones que se dirigen a la totalidad de centros educativos públicos dependientes de la Consejería de Educación, Universidades, Ciencia y Portavocía de la Comunidad de Madrid con la finalidad de proporcionarles un marco de actuación que les permita gestionar la información personal con las mayores garantías posibles para la privacidad de los interesados.

También, como ayuda, la Delegación de Protección de Datos de la Consejería pone a disposición de todos los centros educativos modelos, informes y recomendaciones en su página web https://dpd.educa2.madrid.org

Ante cualquier duda, los centros educativos pueden dirigir sus consultas a la Delegación a través de su dirección de correo:

protecciondatos.educacion@madrid.org – **91 720 4068**

En el ámbito educativo público la responsabilidad del tratamiento de los datos recae en las autoridades educativas, y esto es algo que deben tener siempre presentes los centros educativos públicos. Por este motivo el presente documento ha sido revisado y autorizado por las Direcciones Generales competentes en todos y cada uno de los ámbitos educativos en los que es competente la Consejería de Educación, Universidades, Ciencia y Portavocía[1]. Por lo que respecta al uso de las plataformas y medios técnicos, también ha sido supervisado y autorizado por la Dirección General competente en la elaboración de directrices de uso de las plataformas informáticas de los centros educativos y sistemas informáticos vinculados al aprendizaje y actualización docente[2].

Madrid, 2021

[1] Dirección General de Educación Infantil, Primaria y Especial, Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial y Dirección General de Universidades y Enseñanzas Artísticas Superiores.
[2] Dirección General de Bilingüismo y Calidad de la Enseñanza

Tabla de contenido

1. Recogida y tratamiento de datos por los centros educativos

La disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE), en lo relativo a los datos personales de los alumnos, otorga a los centros la potestad de recabar los datos de su alumnado que sean necesarios para el ejercicio de su función educativa.

Asimismo, establece que los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información.

La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad.

En todo caso, la información será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

En consecuencia, se podrá solicitar, **sin necesidad de consentimiento** de los alumnos mayores de edad o de los tutores legales de los menores los datos relativos:

- Al origen y ambiente familiar y social, las características o condiciones personales, el desarrollo y resultados de su escolarización y en general las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.
- Los datos de salud que sean necesarios para el ejercicio de la función educativa y relacionados con el desempeño académico del alumnado (discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias o alergias); también el tratamiento médico que reciba un alumno a través del servicio médico o de enfermería que corresponda o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.
- Datos biométricos, como puede ser la utilización de la huella dactilar para finalidades como el control de acceso al servicio de comedor en centros escolares con un gran número de alumnos, siempre que se adopten medidas que refuercen la confidencialidad de los datos como la conversión de la huella a un algoritmo, el cifrado de la información, la vinculación a un dato distinto de la identificación directa del alumnado o la limitación de los protocolos de acceso a los datos.
- Las fotografías a los efectos de identificar a cada alumno en relación con su expediente.
- Grabaciones de los alumnos con fines educativos.

No obstante, con carácter previo al tratamiento, se debe cumplir con el derecho de información del alumnado o de sus tutores legales, proporcionándoles la correspondiente política de privacidad.

Procedimiento de recogida

Siempre que vayan a recogerse datos personales es necesario informar a los interesados sobre cómo será el tratamiento de sus datos. La información puede facilitarse al pie del formulario de recogida de los datos, en cartelería en el centro educativo en un lugar visible, en la página web del centro etc.…

Cuando sea necesario recabar el consentimiento informado de los interesados, este siempre se debe incluir en el mismo impreso o formulario en el que se recaban los datos, junto con la información sobre protección de datos.

2. Publicación de listados y comunicación de calificaciones

Publicación de listados en general

En general, las publicaciones de listados deberán realizarse en un entorno seguro como el de EducaMadrid al que sólo se pueda acceder mediante usuario y contraseña, por ejemplo, el Aula Virtual o una carpeta compartida en la nube o Cloud de EducaMadrid o como el módulo Roble de Raíces. Si esto no fuera posible las publicaciones deberán realizarse en tablones de anuncios alojados en el interior del centro, y suficientemente alejados de las puertas principales de los edificios.

Cuando deban publicarse listados cuyos afectados carecen de usuario y contraseñas registrados, mientras no se disponga de un sistema de secretaría virtual para todos los procedimientos que requieran la publicación de datos, debe evitarse el acceso abierto y sencillo dentro de la página web y, preferentemente, se comunicará una contraseña de acceso al listado a todos los interesados en el procedimiento.

Por ello, no deberán publicarse listados en abierto en las páginas web de los centros. En ningún caso podrá aparecer el nombre y dos apellidos junto con el DNI completo, este dato personal evitará publicarse siempre que sea posible y no lo exija la normativa aplicable al procedimiento. Para anonimizar cualquier número de identificación personal (DNI, NIA…) se deberá atender al criterio establecido por la Agencia Española de Protección de Datos en su “Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD”.

- Es decir, siempre que sea posible se incluirá únicamente el nombre y los apellidos y se publicará en un lugar preferentemente restringido donde haya que acreditarse mediante contraseña.

- Cuando esto no sea posible la publicación se hará de modo que el acceso se realice a través de múltiples enlaces.
- Cuando sea necesario publicar nombre y apellidos junto al DNI, este se enmascarará.

Publicación de listados de admisión

Tanto el Decreto 29/2013, de 11 de abril, del Consejo de Gobierno, de libertad de elección de centro escolar en la Comunidad de Madrid, como la Orden 1240/2013, de 17 de abril, de la Consejería de Educación, Juventud y Deporte, establecen la obligación de hacer pública la lista de admitidos, de acuerdo con el principio de publicidad establecido por la Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas, pues se trata de un procedimiento de concurrencia competitiva. Sin embargo, para respetar la privacidad de los datos, la consulta en la página web de estos listados provisionales, que contienen información que podría afectar a la intimidad o seguridad de los participantes, siguiendo el criterio de la AEPD en su guía[3], informe[4] y procedimientos sancionadores[5], debe estar restringido a las personas que hayan participado en el proceso, con acceso mediante contraseña.

A este fin, está previsto que antes del inicio del proceso de admisión se elaboren y envíen a los centros instrucciones relativas al procedimiento de publicación de listados mediante la utilización de las herramientas de EducaMadrid.

Publicación de calificaciones

Respecto de la publicidad de las calificaciones, la AEPD señala que las calificaciones de los alumnos se han de facilitar a los propios alumnos y a sus padres. En el caso de comunicar las calificaciones a través de plataformas educativas, éstas sólo deberán estar accesibles para los propios alumnos, sus padres o tutores legales, sin que puedan tener acceso a las mismas personas distintas. No se recomienda comunicar en voz alta las de calificaciones en el aula.

[3] Guía para centros educativos, la AEPD en la página 27 se refiere a la publicidad de alumnos admitidos, señalando expresamente que "*la publicidad deberá realizarse de manera que no suponga un acceso indiscriminado a la información, por ejemplo, publicando la relación de alumnos admitidos en los tablones de anuncios en el interior del centro o* ***en una página web de acceso restringido a quienes hayan solicitado la admisión***."

[4] Informe jurídico 2021-0013_Publicación productividad individual personal funcionario la AEPD también se ha pronunciado sobre la necesidad de que la publicación se realice de manera restringida y no en abierto.

[5] A la Consejería de Educación, Universidad y FP de Cantabria PS 00024-2019 **por publicar en abierto datos de admisión en la página web de los centros educativos**, al Ayuntamiento de El Escorial con fecha 11/05/2021, PS 00347-2021 y A la Junta de Extremadura, con fecha 24/03/2021, PS 00147-2021,

Por ello, la forma más adecuada y segura de compartir información o datos personales, entre profesores o entre profesores y alumnos es el uso del Aula Virtual, donde la información confidencial relativa a exámenes, contenidos educativos o calificaciones sólo estará accesible a los propios alumnos o a sus padres o tutores legales mediante sus credenciales, sin que puedan acceder personas distintas.

La información que deba proporcionarse a las familias deberá comunicarse a través de los medios oficialmente establecidos, como ROBLE, el Aula Virtual o carpeta compartida de Cloud, donde las calificaciones sólo estarán accesibles a los propios alumnos o a sus tutores legales mediante sus credenciales, sin que puedan acceder personas distintas.

3. Custodia, confidencialidad y compartición de documentos

Para evitar poner en riesgo la seguridad y confidencialidad de la información y la privacidad de los datos, el personal del centro educativo deberá tener especial cuidado en la custodia y transporte de documentos que contengan datos personales, así como los entregados por los alumnos en forma de trabajos, pruebas o exámenes. La forma más segura de conservarlos es digitalizarlos y alojarlos en el Aula Virtual o en la nube de EducaMadrid, devolviendo a sus titulares los originales que hayan sido presentados en papel. Para documentos con información de carácter administrativo la opción adecuada es alojarlos en las plataformas corporativas de gestión (RAICES o SICE).

Los documentos originales en papel, después de digitalizados, deberán bien devolverse a sus titulares, bien remitirse al archivo y, mientras tanto, custodiarse bajo llave y actuar con diligencia mediante una política de mesas limpias para evitar que queden al alcance de terceros (por ejemplo, no dejarlos encima de una mesa al finalizar la jornada, etc.).

Cuando se precise consultar algún documento en formato papel que contenga datos personales o confidenciales, es conveniente que sea digitalizado cuanto antes para evitar acceder a él de nuevo de manera presencial y ubicarlo en medios de compartición de la plataforma Raíces, la nube de EducaMadrid, el aula virtual o la mediateca con acceso mediante credenciales.

En este sentido, el artículo 53.1 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, se refiere al tiempo de conservación y destrucción de documentos.

En resumen, establece que los documentos presentados por el interesado en soporte papel o en formato electrónico dentro de un dispositivo que por cualquier circunstancia

no le puedan ser devueltos en el momento de su presentación, una vez digitalizados serán conservados a su disposición durante seis meses para que pueda recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

Transcurrido el plazo previsto, la destrucción de los documentos se realizará de acuerdo con las competencias del Ministerio de Cultura y Deporte o del órgano competente de la comunidad autónoma, y siempre que no se trate de documentos con valor histórico, artístico u otro relevante o de documentos en los que la firma u otras expresiones manuscritas o mecánicas confieran al documento un valor especial.

Los documentos originales o copias auténticas de documentos en soporte no electrónico se restituirán a sus oficinas, archivos o dependencias de origen, donde les será de aplicación la normativa específica en materia de archivos y conservación del patrimonio documental en su respectivo ámbito y siguiendo lo establecido por las autoridades calificadoras que correspondan.

En especial deberá evitarse el uso de dispositivos de almacenamiento extraíble (pendrive USB, CD, etc.), así como remitir documentos con datos personales por correo electrónico y, menos aún, mediante el uso o redirigiendo los mensajes a una dirección personal no corporativa.

En el caso excepcional de que no exista otra alternativa y haya que emplear el correo electrónico como última opción la información deberá cifrarse y en ningún caso se transportará junto con la contraseña de descifrado. La contraseña de descifrado deberá comunicarse al interesado mediante otra vía como puede ser el teléfono u otro mensaje de correo distinto.

Véanse las guías publicadas a este respecto en la página web de la Delegación de Protección de Datos y de Madrid Digital:

Envío de datos personales a terceros y Transporte de documentos de forma segura (técnicas de cifrado)

Compartición de datos personales empleando la nube (Cloud) de EducaMadrid (útil, por ejemplo, para compartir imágenes o videos con las familias)

Madrid Digital - Documentos y equipos fuera de la oficina.

Madrid Digital - Recomendaciones para evitar el Phishing.

4. Notificación de brechas de seguridad

Cuando se detecte una brecha de seguridad, el centro educativo deberá informar inmediatamente a la Delegación de Protección de Datos en la dirección de correo electrónico y teléfono señalados al inicio y a las autoridades educativas. El director del centro deberá recabar la información de lo acontecido y reflejarlo en un informe, para lo que podrá contar con el apoyo y guía de la Delegación. Debe comunicarlo inmediatamente ya que la Delegación de Protección de Datos deberá notificar a la AEPD en el plazo de 72 horas. Para saber si es necesario notificar a este organismo, en su página web se encuentra la herramienta "Comunica-Brecha RGPD".

5. Obtención del consentimiento informado

Para garantizar el derecho a la protección de datos personales, **los centros educativos deben informar en todo caso del tratamiento de datos personales que de ellos realizan** de la forma en que detalla el RGPD.

Es necesario recabar el consentimiento previo de los alumnos mayores de 14 años o de sus representantes legales en el caso de alumnos menores de esa edad, informando previamente sobre aquel, cuando se solicitan datos personales para otras finalidades legítimas distintas a las estrictas de la función educativa y generalmente de carácter voluntario, están son algunas actividades por las que sería necesario solicitar consentimiento:

- Para la publicación de imágenes y videos en la página web del centro, en redes sociales, en la revista del centro….
- Para enviar información institucional o de publicidad de actividades realizadas por el centro.

Este consentimiento informado deberá ser confeccionado de acuerdo con los siguientes parámetros:

- Debe ser un consentimiento informado, significa que ha de informarse acerca de qué datos se recaban, cómo se tratan, para qué fines o usos, a quien/es podrían ser objeto de cesión.
- Específica, es decir hay que especificar para qué finalidades se presta el consentimiento de forma diferenciada, los interesados deben poder elegir si consienten el uso de las imágenes para redes sociales, revista del centro, página web…
- Los formularios en los que se presta el consentimiento se conservarán durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

Para facilitar esta labor la Delegación de Protección de Datos ha puesto a disposición de los centros los siguientes modelos oficiales de prestación de consentimiento.

El centro educativo, en la primera reunión de tutoría con los padres o tutores legales, deberá explicar el contenido y alcance de la información sobre protección de datos incluida en los modelos de consentimiento. Dicho contenido, adaptado a su edad y conocimientos, también deberá darse a conocer a los alumnos desde el principio del curso para iniciar su formación y concienciación en dicha materia y conseguir inculcar el uso responsable, crítico y seguro de las tecnologías en relación con sus datos personales, sin perjuicio de que a lo largo del curso el centro deba recabar el consentimiento para actividades no previstas al inicio.

En el caso de autorizaciones para asistir a cualquier tipo de actividad voluntaria, como la visita a un museo, donde se autoriza por los padres o tutores legales la asistencia a la actividad de alumnos menores de edad, no se autoriza el tratamiento de los datos por parte de la empresa u organismo que presta el servicio. **Solo es necesario informar del tratamiento de datos en el formulario donde estos se recogen**, ya que generalmente es necesario comunicarles los datos para que el servicio se preste con normalidad. Pensemos en el caso de una actividad en un parque acuático. Si un alumno se lesiona, el seguro que cubre esta contingencia exige conocer la lista de alumnos que asistieron.

6. Uso de aplicaciones y plataformas educativas

Antes de implantar el uso de una aplicación o plataforma educativa en el centro se recomienda por parte de la Delegación de Protección de Datos reflexionar sobre si la medida es necesaria o no, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. El término necesidad no debe confundirse con utilidad sino si el uso de esa aplicación o plataforma educativa es objetivamente necesario para la finalidad que se pretende. Es preciso analizar si su implementación es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés del centro que perjuicios sobre otros bienes o valores en conflictos como puede ser la privacidad de los datos del alumno o su huella digital.

Con carácter general no se autoriza la utilización de plataformas o herramientas educativas distintas de las aplicaciones oficiales de gestión digital para finalidades administrativas o de gestión de los centros educativos, que deberán realizarse con las aplicaciones oficiales de gestión digital y que requiere que los alumnos o sus representantes legales dispongan de los accesos necesarios para interactuar también de manera digital en los trámites en los que estos deban intervenir.

En la gestión de la actividad docente mediante el uso de herramientas y plataformas educativas, los centros educativos deberán atenerse a los siguientes criterios:

1. En primer lugar, los centros educativos deberán emplear para la actividad docente las herramientas y recursos tecnológicos que la Consejería de Educación, Universidades, Ciencia y Portavocía pone a su disposición en la plataforma de gestión Raíces y en la plataforma educativa corporativa EducaMadrid. Aquí, además de las herramientas propias, se encuentran integradas otras externas a las que se ha autorizado su uso en este entorno seguro.
2. En segundo lugar, para aquellos servicios que no puedan prestarse por EducaMadrid se podrá hacer uso de otros recursos complementarios que la autoridad educativa habilite como tales, y que serán incluidos en la página https://www.educa2.madrid.org/recursos.
3. Y, por último, cuando los centros educativos públicos deseen emplear aplicaciones educativas que no figuran en los párrafos anteriores, deberán solicitar autorización y supervisión a la Consejería de Educación, Universidades, Ciencia y Portavocía. **Deberán abstenerse de emplear aplicaciones o plataformas educativas no corporativas o no consideradas por la Consejería como complementarias que exijan adherirse a las condiciones del prestador del servicio, y que no permitan suscribir un contrato de encargo de tratamiento.** Tampoco deberán hacerlo si no son capaces de garantizar y poder demostrar el estricto cumplimiento de la normativa vigente sobre protección de datos. Es muy importante que el centro compruebe previamente que no existen recursos en Raíces o EducaMadrid que permitan ofrecer prestaciones similares, ya que estas primarán sobre el uso de la herramienta ajena en relación con la privacidad de los datos.

Cuando un centro educativo desee emplear una aplicación o plataforma educativa no corporativa o no complementaria **deberá elaborar con carácter previo un proyecto detallado sobre el tratamiento de los datos personales que pretende introducir en ellas**, para su posterior evaluación de impacto sobre la privacidad y validación por la D.G. de Bilingüismo y Calidad de la Enseñanza, que contará con el asesoramiento de la Delegación de Protección de Datos.

El proyecto contendrá, al menos, lo siguiente:

- Justificación de las funcionalidades que ofrece la aplicación que no pueden obtenerse de EducaMadrid o de las plataformas declaradas como complementarias.

- La evaluación de impacto realizada cuando se trate de datos de menores de edad.
- Descripción del modo en el que se utilizará la aplicación en lo referente a los datos de los interesados, explicando claramente la información que podrá ser tratada y las medidas para su anonimización o seudonimización. En este caso, el centro deberá asegurarse de que las posibilidades de reidentificación, directamente o mediante fuentes de datos accesibles, son limitadas y asumibles.
- **La aplicación nunca se utilizará para tratar datos de carácter administrativo con efectos jurídicos,** como la **gestión de faltas** de asistencia de alumnos y profesores, **tramitación de bajas** laborales, **gestiones económicas**, evaluación de pruebas de conocimiento o aptitud, ya sean estas parciales o finales, **valoración de conductas o procedimientos disciplinarios, pruebas de tipo psicopedagógico y cualquier otro trámite de carácter confidencial corporativo**, incluidas las aplicaciones del tipo **"cuadernos del profesor" o equivalentes**, ya que todas estas actividades deben realizarse mediante las herramientas corporativas.
- La aplicación se utilizará como una herramienta más dentro de la función educativa, asociada a un ámbito o una asignatura, materia o módulo, para potenciar y perfeccionar el aprendizaje. El grupo de alumnos y el profesor serán los únicos partícipes en el uso de dicha herramienta, cuyos datos estarán preferentemente anonimizados o seudonimizados y se limitarán a los mínimos posibles.
- Los trabajos que se materialicen como fruto de su uso, si deben conservarse, se alojarán en el aula virtual, mediateca o nube de EducaMadrid y se conservarán como cualquier otra que tuviese formato papel, por el tiempo necesario, debiendo ser borrados o no grabados en la aplicación externa.
- Los trabajos o pruebas nunca serán difundidos ni publicados a través de la aplicación, ya sea esta institucional o ajena, ni por los profesores ni por los alumnos.
- Los profesores y los padres o tutores legales serán informados de la actividad realizada por sus hijos a través de los medios corporativos y nunca mediante acceso a través de la aplicación externa y menos aún mediante el uso de redes sociales o mensajería instantánea. Tampoco debe hacerse a través del correo electrónico, salvo excepcional necesidad y, en este caso, el documento debe ir cifrado.
- Cuando el alumno o sus representantes legales en el caso de un menor de 14 años ejerzan su derecho de oposición motivadamente al tratamiento de sus datos personales mediante estas herramientas, el centro deberá tener en cuenta lo siguiente:

  - El centro educativo deberá garantizar por escrito que el alumno va a recibir las mismas atenciones con una efectividad educativa equivalente mediante los medios corporativos al alcance del centro, sin que ello suponga para el alumno ningún tipo de discriminación frente al resto de alumnos que sí utilizarán la aplicación.
  - Si, tras explicar esto con claridad al alumno y a sus padres o tutores legales, el centro constata la imposibilidad de garantizar la no discriminación de aquel, el centro educativo deberá cesar en su intención de utilizar la aplicación con el grupo de alumnos. En su explicación es preceptivo que el centro informe a los padres o tutores legales del alumno de que, en caso de que no queden conformes con la decisión del centro, estos están en su derecho de reclamar al respecto ante la autoridad nacional de protección de datos (AEPD).

- La política de seguridad de la aplicación deberá ser completa, inteligible y fácilmente accesible.
- Los servidores donde se almacenan los datos personales deben estar en el UE o en el caso de existir transferencias internacionales asegurarse que se garantizan las medidas de seguridad adecuadas que permitan la transferencia internacional.

Se deben elegir proveedores que facilitan información de forma transparente y clara que nos permita conocer dónde se encuentran sus servidores y en caso de que existan transferencias internacionales el proveedor deberá adoptar medidas de seguridad adicionales, como códigos de conducta o cláusulas contractuales tipo.

Cuando el centro haya sido autorizado para utilizar aplicaciones o plataformas con fines educativos, **deberá <u>previamente</u> informar con claridad** a todos los interesados sobre las condiciones y restricciones de uso que apliquen y sobre la política de seguridad:

- identidad y dirección del responsable: Dirección General competente,
- finalidades para las que serán utilizados los datos,
- posibles comunicaciones de datos a terceros y su identidad,
- finalidad para la que se ceden,
- derechos que asisten a los titulares de los datos, ubicación de los datos,
- periodos de conservación,
- medidas de seguridad facilitadas por la aplicación y posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores

Además, debe poder demostrar documentalmente que ha informado convenientemente a los interesados e **incorporar toda esta información en la PGA**.

7. Redes sociales y publicaciones en Internet

Los centros docentes se abstendrán de publicar datos personales o contenidos audiovisuales que identifiquen o permitan identificar sin dificultad a los alumnos en modo abierto (páginas web públicas, redes sociales, etc.), con el fin de no contribuir con ello a la formación de la huella digital de las personas.

Aunque la normativa sobre protección de datos determina que dicha publicación en abierto puede realizarse si se cuenta con el consentimiento informado del alumno o de sus representantes legales cuando este es menor de 14 años, los centros docentes deben tener en cuenta que este tipo de publicaciones puede afectar negativamente a los alumnos en el futuro. Por tanto, antes de publicar la imagen de un alumno en redes sociales se recomienda reflexionar sobre la finalidad de la publicación de la foto, es decir, cual es el objetivo por el que se desea compartir esa imagen:

- Si la finalidad es compartir con las familias de los alumnos la vida del alumno en la escuela, sus actividades educativas o extraescolares, sus trabajos, en definitiva, cualquier actividad que pudiera ser de interés para las familias, se recomienda que se haga bien a través de Roble, que se encuentra dentro de la plataforma corporativa Raíces, bien compartiendo el contenido en el Aula virtual o bien en la nube de EducaMadrid, ya que en todas ellas se accede mediante usuario y contraseña a un espacio seguro y al que solo pueden acceder los destinatarios a los que se quiere hacer llegar las imágenes.

- Si, por el contrario, la finalidad de la publicación es dar a conocer aspectos del su funcionamiento del centro y las actividades que se realizan para promoción del centro educativo, en ese caso no es preciso que aparezcan las imágenes de los alumnos y podría llevarse a cabo en abierto sin ningún problema, siempre que no se identifique a los alumnos, aparezcan fotos de lejos, de espalda, sus manos trabajando…

Para la captación de imágenes o vídeos dentro o fuera del centro no se permite el uso de dispositivos móviles privados de los profesores u otro personal del centro educativo.

Véase el documento: Recomendación dirigida a los centros educativos para no publicar imágenes cuando no es necesario.

8. Publicación de información académica y/o del alumnado en blogs del profesorado mensajería instantánea, redes sociales o páginas web

El blog del profesorado es un recurso didáctico utilizado como medio de información y comunicación complementario y voluntario en su función docente.

No se podrán publicar en el blog de un docente datos de carácter personal que permitan identificar al alumnado. Tampoco deberá hacerlo a través de mensajería instantánea, redes sociales o páginas web.

De forma análoga a los blogs de los centros educativos, se podría publicar la información previa disociación o anonimización de los datos del alumnado de manera que no se les pueda llegar a identificar.

Por otro lado, cuando la grabación se realiza dentro del centro por familiares o amistades del alumnado o por el profesorado fuera de su actividad docente, como por ejemplo, en la fiesta de Navidad o fin de curso, carnavales, jornadas culturales, etc., su destino será exclusivamente para el uso en el ámbito personal, familiar y de amistad, siendo los autores y receptores de las grabaciones los únicos responsables del uso inadecuado de las mismas, como puede ser la publicación de contenido audiovisual sin el consentimiento de personas ajenas que figuren en el mismo.

9. Obligación de encender la cámara en las clases en línea.

La imagen de los alumnos y profesores que se puede visualizar durante las clases en línea es información personal y por tanto se le aplica la normativa sobre protección de datos. El tratamiento debe ser lícito y estar fundamentado en algunas de las bases del artículo 6.1 del RGPD, concretamente en los apartados c), obligación legal para el responsable, y e), misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. Además, debe tener una finalidad concreta y necesaria para el ejercicio de dichos poderes públicos.

La norma que habilita el tratamiento en nuestro caso es la Ley Orgánica 2/2006, de 3 de mayo de Educación (LOE), cuando establece que los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa, teniendo en cuenta que la incorporación de un alumno en un centro docente supondrá el tratamiento de sus datos.

Sin embargo, en el tratamiento de los datos del alumnado se aplicarán normas técnicas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afectan al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

El tratamiento de la imagen en el ámbito educativo se tiene que contextualizar en una situación que lo haga necesario, como en el caso de la pandemia por COVID-19,

cuyos efectos perduran y aún puede ser necesario que muchos alumnos no asistan a las aulas de manera presencial cuando se detecta un caso positivo. Pero también puede ser necesario en actividades con niños con alguna discapacidad, necesidades especiales o situación de vulnerabilidad, como puede ser una enfermedad prolongada.

En todos estos casos es necesario aplicar medidas de aprendizaje alternativo a la presencialidad de los alumnos y resulta lícito conforme al RGPD que los profesores puedan visualizar y, por tanto, tratar la imagen de sus alumnos para poder comunicarse e interaccionar con ellos en el ejercicio de la función educativa.

El docente ha de tener contacto visual con los alumnos para identificarlos y confirmar su asistencia remota a la clase. Pero a esto hay que añadir que la visualización del alumno por parte del docente durante la clase permite una interacción más ágil con ellos para facilitar y hacer viable el desarrollo de la sesión. Por lo tanto, desde el punto de vista de protección de datos, un profesor puede instar a sus alumnos a mantener la cámara activada durante la clase en línea y permitir que el docente pueda mantener el contacto visual con ellos.

No obstante, los profesores deben cumplir con el resto de principios sobre protección de datos, sobre todo con el **principio de minimización**, que exige que los responsables traten sólo los datos personales que sean “adecuados, pertinentes y limitados a aquello necesario en relación con las finalidades del tratamiento” (artículo 5.1.c) RGPD). Por ello, los centros educativos deben determinar si en algunos casos el normal desarrollo de la clase en línea hace innecesario mantener la visualización constante con el alumno por parte del docente.

Íntimamente relacionado con este principio se encuentra el de **proporcionalidad**, que nos insta a ponderar si, aun siendo lícito, el tratamiento está siendo o no desproporcionado. Es decir, es razonable que al empezar la sesión el docente debe tener un contacto visual con el alumno para confirmar su asistencia a la clase en línea, pero se debe considerar la necesidad de mantener la cámara activada durante toda la sesión y en qué contexto es necesario.

También debemos tener en cuenta otros factores:

- **La edad de los alumnos**. Cuando los alumnos son de corta edad el profesor necesita comprobar que el alumno sigue y entiende las explicaciones correctamente y puede ser pertinente el contacto visual continuo con ellos. Pero con alumnos de más edad podría ser suficiente la interacción a través del chat o de la voz.
- **La naturaleza de la actividad**. En actividades de tipo participativo puede ser más relevante disponer de manera continuada de la imagen de los alumnos, mientras

que en otro tipo de actividades puede ser suficiente una visualización puntual a través de la cámara.

Hay que apreciar que la captación continuada de la imagen del alumno puede ser altamente invasiva, ya que no en todos los casos se podrá garantizar que el espacio donde se encuentra el alumno está exclusivamente a su disposición y que pueden interactuar otros miembros de su familia, sobre todo si se mantiene activado el sonido.

Por ello es importante que los alumnos conozcan desde las primeras etapas de adquisición de sus competencias digitales la forma en que deben activarse las medidas de privacidad, como aplicar un fondo neutro a su imagen y el control de la cámara y el micrófono.

También se debe aplicar el principio de proporcionalidad, inherente al principio de minimización cuando se decide grabar la sesión, donde habría que descartar la grabación de los alumnos mientras se imparte la clase, aunque puede ser adecuado o necesario en circunstancias concretas, como en la realización de una prueba, cuestión que se aborda en el apartado siguiente.

Por otro lado, cabe plantearse si los alumnos se pueden negar a tener la cámara activada alegando su derecho de imagen o el impacto en la privacidad de su domicilio, aunque impartir clases en línea no implique un tratamiento de datos personales de especial protección.

En el desarrollo de una clase presencial, el contacto visual continuo del docente con los alumnos no representa una intromisión en su imagen o su privacidad, ya que la clase se lleva a cabo en el ámbito restringido del aula con un impacto menor sobre la imagen.

En cambio, la clase en línea desde el domicilio del alumno supone otros condicionantes, como disponibilidad de un espacio propio, compartirlo con otras personas, etc., que podrían afectar en mayor medida a la intimidad de ciertos alumnos.

En cualquier caso, la normativa de protección de datos prevé que los afectados, los profesores, los alumnos de los centros escolares o sus padres o tutores legales puedan ejercer su derecho de oposición (artículo 21.1 RGPD): **El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular**, a que sean tratados sus datos personales. **El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado**, o para la formulación, el ejercicio o la defensa de reclamaciones,

Los alumnos tienen la opción de oponerse a la captación de su imagen durante las clases en línea y el responsable debe atenderlo sin que se produzca menoscabo en sus derechos o en la calidad del servicio proporcionado, de manera que si este no tiene motivos legítimos imperiosos que justifiquen el mantenimiento del tratamiento,

tiene que dejar de hacerlo, y el alumno podrá seguir la clase en línea sin que su imagen sea captada.

En conclusión, en principio el profesor puede instar a los alumnos a tener la cámara activada durante la clase en línea si resulta necesario para el desarrollo de la clase, sin perjuicio del ejercicio legítimo del derecho de oposición por parte de los afectados, que se tendrá que atender y resolver en atención a lo que dispone la normativa (art. 21 RGPD).

Sin embargo, lo que el responsable no puede dejar de hacer es informar del tratamiento a las personas afectadas, a fin de que puedan conocer con claridad la finalidad para la cual se pretende realizar este tratamiento, cuál es la base jurídica que permite llevarlo a cabo, y la posibilidad de ejercer los derechos que prevé la normativa de protección de datos, entre otras cuestiones, en los términos previstos en el artículo 13 del RGPD.

Véase el dictamen de la Autoridad Catalana de Protección de Datos CNS 11/2021,

10. Grabaciones audiovisuales efectuadas en los centros educativos

En el ejercicio de la actividad educativa los centros disponen de nuevas herramientas que permiten impartir la docencia y evaluar a los alumnos de forma remota. El uso de herramientas de evaluación que conllevan la implantación de sistemas de reconocimiento facial o herramientas antiplagio, así como la grabación de las pruebas de evaluación realizan tratamientos que implican una mayor intrusión en el derecho a la protección de datos y que han conducido a la AEPD a adoptar criterios en este sentido en su informe jurídico 2020-0036.

La grabación es una actividad más invasiva que la retransmisión en remoto por lo que es preciso analizar las siguientes cuestiones:

- En primer lugar, analizar **si la medida es necesaria** o no, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. Es, decir, si la grabación es objetivamente necesaria para la finalidad que se pretende, no si solamente es útil.
- En segundo lugar, es preciso analizar **si su implementación es ponderada** o equilibrada por derivarse de ella más beneficios o ventajas para el interés que perjuicios sobre otros bienes o valores en conflictos.
- Utilizar la videoconferencia para impartir una clase o realizar un examen, así como grabar su contenido no requiere del consentimiento del alumnado o de sus padres o tutores legales, pero sí comporta la obligación de informar sobre esta circunstancia a los interesados, además de quién es el responsable, la legitimación y finalidad, que deberá motivarse, las cesiones o transferencias

internacionales que pudieran realizarse, la forma y periodo de conservación de la información que se genere, así como el ejercicio de derechos.

- Para evitar perder el control solamente el profesor debe grabar la sesión, conservando la grabación durante un tiempo limitado al estrictamente necesario y con el contenido educativo relevante, evitando grabar a los alumnos. Las grabaciones de imagen y voz solamente deben ser del profesor, que evitará grabar las intervenciones de los alumnos.
- La grabación de pruebas de conocimiento, aptitud o exámenes de todo tipo realizados de manera motivada y proporcionada debe estar a disposición de los alumnos o sus padres o tutores legales para posibles reclamaciones o ejercicio de derechos, dado que estas pruebas están reconocidas por el TJUE como datos personales.
- Por cuestiones de confidencialidad y de privacidad, la forma más segura de conservar las grabaciones es hacerlo mediante acceso restringido al Aula Virtual o a la nube corporativa (Cloud de EducaMadrid), solo a las personas autorizadas para consultar o manejar esa información y conservándolas durante el tiempo estrictamente necesario.
- Dicha información, como ya se ha indicado en el apartado correspondiente al uso de aplicaciones externas, no se alojará en nubes o servidores no autorizados por la Consejería ni en dispositivos locales, tanto profesionales como personales, pues en caso de pérdida, extravío o acceso no deseado, podría producirse una brecha de seguridad que habría que comunicar a la Agencia Española de Protección de Datos. Para la grabación únicamente deben utilizarse las aplicaciones que con este fin la Consejería haya puesto a disposición de los centros educativos.

Asimismo, se recomienda seguir las siguientes reglas en el uso de herramientas para videoconferencia con el fin de no poner en riesgo la privacidad, confidencialidad y seguridad de los datos:

- ✓ Si la herramienta no permite la grabación de la sesión, debe informarse a quienes van a participar en ella que no deben grabar con sus propios dispositivos el contenido de esta. **Es importante informar a menudo**, a través de carteles o mensajes, **de la responsabilidad en que se incurre cuando no se hace un uso adecuado** de la información o de los datos personales, y que se puede cometer una infracción sancionable por la Agencia Española de Protección de Datos.
- ✓ **Si la sesión va a ser grabada, es muy importante evitar el uso de medios personales y procurar utilizar los corporativos que no tengan activada la**

sincronización en línea, con el fin de impedir que la grabación se aloje en servidores extraños.

- ✓ No debemos utilizar las herramientas de videoconferencia fuera del entorno de EducaMadrid o de acceso sin estas credenciales en plataformas consideradas complementarias, es decir, no debemos acceder a ellas mediante la fórmula gratuita para cualquier tipo de usuario.

Para más información, véase los informes de la Delegación de Protección de Datos y de Madrid Digital:

Informe para la realización de actividades educativas no presenciales por medios telemáticos en los centros educativos de la Comunidad de Madrid con respecto a la privacidad.

Informe sobre la legalidad de las grabaciones efectuadas en centros educativos

Informe sobre la obligación por parte de los profesores de utilizar determinadas herramientas para impartir la docencia en remoto

Ciberseguridad: Videollamadas y reuniones virtuales.

Recomendaciones para las videollamadas y reuniones virtuales.

Otros informes de interés:

Guía de recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León

Resumen de la Segunda Jornada Online para Compartición de Experiencias de Modelos de Evaluación

11. Grabaciones de las sesiones de los órganos colegiados

De acuerdo con la Ley Orgánica de Educación, los órganos colegiados de constitución obligatoria en los centros educativos son el Claustro de profesores y el Consejo Escolar, pero tienen la consideración de órgano colegiado por su forma de funcionamiento cualquier otro órgano de coordinación docente, como las juntas de evaluación, comisiones de coordinación o departamentos didácticos, de acuerdo con la Ley 40/2015 del Sector Público, podrán convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas tanto **de forma presencial como a distancia**.

En las sesiones celebradas **a distancia**, sus miembros podrán encontrarse en distintos lugares **siempre y cuando se asegure por medios electrónicos** la

identidad de los miembros y el contenido de sus manifestaciones, entre otros aspectos. Se considerarán incluidos entre los **medios electrónicos válidos las videoconferencias.**

La AEPD no considera adecuado el consentimiento como fórmula de legitimación de las grabaciones que se lleven a cabo en las reuniones del Claustro o el Consejo Escolar, ya que además de requerir que sea otorgado por todos y cada uno de los participantes, puede ser revocado en cualquier momento, por lo que debe examinarse si la legitimación del tratamiento puede fundarse en alguno de los otros supuestos.

Por ejemplo, si la grabación de los datos está recogida en las normas de funcionamiento del órgano colegiado esta norma vincula a todos sus miembros como resultado de la relación establecida entre el órgano de participación de la comunidad escolar y sus miembros. Sin embargo, dado que la grabación es opcional para los órganos colegiados, **la decisión de grabar o no las sesiones se adoptará, como cualquier otro acuerdo, por mayoría de votos** del órgano correspondiente. En este sentido, el artículo 15.2 de la Ley 40/2015 permite que se completen sus normas de funcionamiento, sin perjuicio del derecho de oposición que pudiera ser ejercido por los afectados. Por ello, como norma que ampara la grabación de las sesiones, los centros educativos cuyos órganos colegiados hayan aprobado este sistema, deben incorporarlo a su Reglamento de Régimen Interior, donde constará la justificación de su uso, la finalidad que persigue, los órganos a los que afecta y las medidas de seguridad para salvaguardar la confidencialidad de la información y la privacidad de los datos personales.

En lo que respecta a la garantía de que los datos personales tratados en las reuniones no se divulguen fuera del seno del órgano colegiado el RGPD establece la responsabilidad de garantizar la confidencialidad de los datos, debiendo adoptarse las medidas necesarias para evitar los riesgos contra la privacidad. No obstante, las deliberaciones que se producen en el seno del órgano no están sometidas al deber de secreto, dado que los miembros se encuentran presentes cuando estas se celebran. Por ello, debe estar garantizado el acceso a favor de los miembros del órgano adoptando las medidas de seguridad necesarias.

Los documentos resultantes de la grabación de las sesiones en soporte electrónico deberán conservarse de forma que se garantice la integridad y autenticidad de los ficheros electrónicos correspondientes y el acceso a los mismos por parte de los miembros del órgano colegiado. Para llevarla a cabo, debería hacerse con medios materiales dispuestos por el centro que garanticen la seguridad, así como la autenticidad e integridad de los ficheros que se creen, evitando el uso de dispositivos personales. Por ello es importante que los centros utilicen preferentemente las

aplicaciones de videoconferencia integradas en EducaMadrid Jitsi y Webex y alojen las grabaciones en su nube o Cloud.

Véase la Sentencia del Tribunal Supremo de 19 de febrero de 2021

Como un tratamiento de datos personales más, debe incorporar su política de privacidad, que se encuentra publicada a disposición de los centros educativos en el apartado "Modelos" de la página web de la Delegación de Protección de Datos.

12. Acceso por el profesorado al contenido de un dispositivo electrónico del alumnado

Dada la información que se contiene en los dispositivos con acceso a internet, así como la trazabilidad que se puede realizar de la navegación efectuada por los usuarios, el acceso al contenido de estos dispositivos del alumnado, incluyendo su clave, supone un acceso a datos de carácter personal que requiere el consentimiento de los interesados o de sus padres o tutores legales si se trata de menores.

No obstante, en situaciones en las que pudiera estar presente el interés superior del menor, como cuando se ponga en riesgo la integridad de algún alumno (situaciones de ciberacoso, "*sexting"*, "*grooming"* o de violencia de género) el centro educativo podría, previa ponderación del caso y conforme al protocolo que tenga establecido, acceder a dichos contenidos sin el consentimiento de las personas implicadas[6].

13. Utilización de aplicaciones de mensajería

Con carácter general, las comunicaciones entre el profesorado y el alumnado deben tener lugar dentro del ámbito de la función educativa y no llevarse a cabo a través de aplicaciones de mensajería instantánea.

En la actividad cotidiana docente, deberá utilizarse los canales, medios y herramientas específicos de comunicación establecidos por la Consejería de Educación, puestas a disposición de profesorado, alumnado y sus tutores legales, como el Aula Virtual o Roble.

Véase a este respecto el informe de la Delegación de Protección de Datos:

[6] Ley Orgánica 1/1996 de Protección Jurídica del Menor: Artículo 2. Interés superior del menor.
1. Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado. En la aplicación de la presente ley y demás normas que le afecten, así como en las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos primará el interés superior de los mismos sobre cualquier otro interés legítimo que pudiera concurrir.

Informe sobre el uso de aplicaciones de mensajería (WhatsApp/Telegram) en el ámbito educativo

14. Publicación de menús en el comedor del centro

En el comedor de los centros educativos se pueden publicar los diferentes menús, ya que puede existir alumnado con necesidades alimentarias especiales, pero sin necesidad de que exista un listado con nombre y apellidos de los alumnos en relación con el menú que le corresponde a cada uno de ellos.

Lógicamente, el centro sí podrá disponer de esos listados para el uso de estos por su servicio de comedor, pero sin darles publicidad.

15. Acceso de los familiares a información sobre ausencias escolares de sus descendientes

Los padres o los tutores legales de los alumnos menores de edad, como sujetos que ostentan la patria potestad, entre cuyas obligaciones está la de educarlos y procurarles una formación integral, tienen acceso a la información sobre las ausencias de sus hijos del centro docente a través de los cauces de información oficiales (como por ejemplo ROBLE).

La AEPD concluye que habrá que examinarse cada supuesto concreto para determinar si existe un interés legítimo en los progenitores para acceder a los datos de los hijos mayores de edad que deba prevalecer sobre los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

En el caso de un interés legítimo demostrado por los progenitores que prevalezca sobre los derechos y libertades fundamentales de su hijo (por ejemplo, dejar de pagar una pensión alimenticia reconocida judicialmente cuando el alumno se matricula únicamente para percibirla sin conseguir resultados positivos), la AEPD señala que estos tendrán derecho a acceder a la información del alumno siempre y cuando aquellos estén sufragando la educación del alumno y su manutención y siempre que del derecho de oposición de este no resulte otra cosa.

No obstante, la AEPD señala que en aquellos casos en los que los progenitores no tengan el consentimiento del hijo mayor de edad y tengan un interés legítimo para la obtención de las calificaciones escolares, deben ponderarse dos elementos fundamentales: el primero, si el tratamiento de los datos es necesario para satisfacer un interés legítimo (del responsable de los datos o del cesionario). El segundo, si han de prevalecer o no los derechos fundamentales del interesado esencialmente referidos a la protección de sus datos personales.

Por ello, ante el caso de un alumno mayor de edad cuyos padres aleguen un interés legítimo para conocer su información educativa (calificaciones, faltas de asistencia, etc.) el centro deberá valorar si no proporcionar la información solicitada puede suponer un riesgo para los intereses vitales del alumno, como su salud o integridad física o psicológica, que sean dignas de proteger por encima de su derecho a la privacidad. En caso contrario, el centro debería inhibirse ante un conflicto de carácter familiar, dado que, si el centro ha valorado que existe un interés legítimo por parte de los padres, debe informar previamente al alumno que va a realizar la cesión de datos, ante la cual el alumno podrá ejercer su derecho de oposición.

Véanse los informes jurídicos de la AEPD 2015-441 y 2017-0141 y TD/02302-2017

16. Comunicación de información escolar del alumnado a sus familiares

Los titulares de los datos personales o quienes ostenten su representación (padres o tutores legales de los alumnos) pueden solicitar información que le afecte en virtud de distinta normativa.

- Conforme al artículo 15 del RGPD, los interesados tendrán derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a estos, a conocer quién es el responsable del tratamiento, la finalidad de este, el origen de los datos y si se van a comunicar a terceros, de los cuales el responsable facilitará una copia. No obstante, el derecho a obtener copia no afectará negativamente a los derechos y libertades de otros, ya que este artículo regula un derecho personalísimo que únicamente permite consultar los datos de su titular o de quienes legalmente representa. Por ello, se censurará en su caso el contenido de los documentos que afecte a otros interesados.
- El derecho de acceso del RGPD es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano. Es decir, este derecho podría dar acceso a datos personales de terceros de acuerdo con el artículo 15 de esta última ley.
- Y es asimismo distinto del acceso a documentos que formen parte de un expediente escolar, salvo aquellos documentos que contengan datos de salud, cuya obtención se habilita en base a la normativa de protección de datos en correlación con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información

y documentación clínica.

- De acuerdo con las Leyes Orgánicas sobre Educación y sus normas de desarrollo, los tutores legales de los alumnos tienen derecho a estar informados sobre el progreso del aprendizaje e integración socioeducativa de sus hijos e hijas, así como estar asesorados e informados para el ejercicio de sus derechos y obligaciones como padres y madres sobre la educación de aquellos. También tienen derecho a obtener copias de determinada documentación relacionada con la actividad docente.

En el expediente académico deben figurar los siguientes documentos y datos:

- ✓ Los datos personales del alumno,
- ✓ Resultados de la evaluación con las calificaciones obtenidas,
- ✓ Las decisiones de promoción o permanencia en la etapa
- ✓ En su caso, las medidas de apoyo educativo y las adaptaciones curriculares que se hayan adoptado.
- ✓ Resultados obtenidos en cuantas pruebas censales de evaluación externa haya participado el alumno
- ✓ Informes psicopedagógicos y médicos
- ✓ Certificaciones expedidas a efectos de convalidaciones, etc.

Es necesario aclarar que toda esta información contiene o son datos personales. Por ello, en aplicación del principio de minimización, **los centros educativos no deberán conservar datos que no tienen que formar parte del expediente académico o que ya no sean necesarios,** como borradores de documentos, autorizaciones, informes, formularios, partes, exámenes, o cualquier otra información obsoleta, puesto que se considera tratamiento la mera conservación de los datos y, en ese caso, los interesados tienen derecho a obtener copia de ellos.

El propio Tribunal de Justicia de la Unión Europea y por ende la AEPD consideran que los exámenes o pruebas son datos de carácter personal y en ellas están incluidas las de carácter psicopedagógico, como las pruebas BADyG, utilizadas para determinar ciertos aspectos o aptitudes relativas al aprendizaje.

La AEPD considera que son datos de salud los informes psicológicos, psicosociales, psicopedagógicos y sus pruebas correspondientes, ya que la evaluación psicotécnica de aptitudes, características de personalidad y preferencias profesionales de los alumnos contiene informaciones concernientes a la salud pasada presente y futura, física o mental, de un individuo.

Así, el alcance del derecho de acceso a los datos de salud se debe ceñir a todos aquellos datos relativos a la determinación y constatación del estado de salud de su titular, ya sea físico o psíquico, pasado, presente y futuro.

En consecuencia, el acceso a estos datos de salud está garantizado conforme al artículo 15 del RGPD. Por esta razón es importante que las pruebas no contengan anotaciones u otro tipo de observaciones que puedan confundir o distorsionar los resultados de las pruebas si son accedidas por personas sin los conocimientos adecuados para interpretarlas.

El derecho de acceso amparado por el artículo 15 del RGPD, es un derecho personalísimo que solo permite al interesado acceder a los datos de los que es titular o de quienes represente legalmente, por ello, los datos personales de terceros que no le afecten serán censurados de manera irreversible en las copias que se le faciliten.

No obstante, a pesar de no tener derecho de acceso, por ejemplo, a los nombres de profesionales invocando el artículo 15 del RGPD, pues este solo permite el acceso a los datos de los que el solicitante es titular, sí podrá tener acceso a ellos acudiendo a la normativa educativa, a la sanitaria, a la de procedimiento administrativo (en la condición de interesado) o en la de acceso a la información pública, y en este sentido los padres tienen derecho a conocer el nombre y número de colegiado. del profesional que ha realizado las pruebas.

Por lo tanto, los centros educativos deben saber que los padres y los alumnos, en virtud de una u otra normativa, tienen derecho a conocer toda la información que el centro custodia o tiene disponible en los sistemas de gestión administrativa o docente. De ahí la importancia de conservar únicamente la información y documentación estrictamente necesaria y relevante que exige la normativa.

Véase la Resolución de la AEPD TD-01233-2018 sobre solicitud de copia de pruebas psicopedagógicas y datos de los profesionales que las realizaron.

17. Acceso por los padres o tutores legales a la información de sus hijos

Los progenitores tienen derecho a recibir la misma información sobre las circunstancias que concurran en el proceso educativo del menor. En la Comunidad de Madrid los centros ponen a disposición de padres o tutores legales esta información en el módulo Roble de la plataforma Raíces, donde cada uno accede con sus propias credenciales.

Cuando alguno de ellos ejerza su derecho de acceso a la información de sus hijos, debemos tener en cuenta que este es un derecho personalísimo que consiste en obtener información sobre el tratamiento que se está haciendo de los datos del propio interesado o de sus hijos cuando ostentan su representación.

Véase la resolución de la AEPD recaída en el expediente TD/00248/2020

La información no debe contener datos personales del otro progenitor, como dirección, teléfono o correo electrónico, aunque sí puede contener ciertos datos de otras personas, como las que están autorizadas a llevar o recoger a los niños al colegio, ya que un padre tiene derecho a conocer si quien se hace cargo de sus hijos es su abuelo, la pareja de la madre o un vecino, aunque no se le proporcione su nombre.

Ambos progenitores tienen el deber de informarse, mutuamente, de todas las cuestiones relevantes que afecten a su hijo, siempre que el conocimiento de aquéllas no lo pueda obtener por sí mismo el progenitor que no esté en compañía del menor en el momento en que las mismas se produzcan (por ejemplo, enfermedad, lo que no sucede en el caso de cuestiones escolares, extraescolares o médicas ordinarias, entre otras, en las que los profesionales que se ocupan del menor tienen la obligación de suministrar, tanto al padre como a la madre, cualquier información que les soliciten sobre su hijo, por ser ambos titulares de la patria potestad. Los progenitores tienen derecho a solicitar y obtener de terceros, personas físicas o jurídicas, públicas o privadas, cuanta información obre en su poder de estos últimos sobre la evolución escolar y académica de su hijo y su estado de salud físico y psíquico.

De esta forma, el centro escolar ha de informar de la misma manera a ambos progenitores de posibles reuniones con tutores, participación en fiestas o festivales escolares, boletines de notas, calificaciones o evaluación, sanciones o absentismo escolar e igualmente tienen derecho a obtener información a través de las reuniones habituales con los tutores y servicios de orientación del centro escolar, tanto si acuden los dos como si lo hacen por separado. Asimismo, el centro de salud o médico de cabecera del menor ha de informar de la misma manera a ambos progenitores de la historia clínica del menor, proporcionar dos copias de los informes, diagnóstico de enfermedades, ingresos hospitalarios, tratamientos prescritos y cualesquiera otras circunstancias relativas a la salud del menor.

Por ello, en caso de conflicto entre los progenitores sobre el acceso a la información académica de sus hijos, estos deberán dirimir la cuestión ante el poder judicial competente en materia de familia, no ante el centro educativo.

Para más información acerca de estos conflictos, véase la Sentencia del Tribunal Supremo de 18 de enero de 2017 (STS 166/2017)

18. Comunicaciones de datos del alumnado

La comunicación de datos requiere, con carácter general, el consentimiento de las personas interesadas, del alumnado o de sus padres o tutores legales si son menores, salvo que esté legitimada por otras circunstancias, como que permita u obligue a ella una Ley, como es el caso de solucionar una urgencia médica, o se produzca en el marco de una relación jurídica aceptada libremente por ambas partes. En estos

últimos supuestos se pueden comunicar los datos sin necesidad de obtener el consentimiento de los afectados.

No se considera comunicación de datos el tratamiento de estos por parte de miembros que forman parte de la organización educativa, aunque no presten sus servicios directamente en el centro escolar, como en el caso de los equipos de orientación que deben valorar circunstancias concretas de su personalidad o aptitudes educativas.

Comunicación de datos de alumnado a otro centro educativo

En caso de traslado, la LOE ampara la comunicación de datos al nuevo centro educativo en el que se matricule el alumnado sin necesidad de recabar su consentimiento o el de sus padres o tutores legales.

Comunicación de datos a otros centros situados en otros países

Se pueden facilitar datos del alumnado de un centro a otra organización en el extranjero para intercambios de alumnado o estancias temporales dado que el acceso a los datos del alumnado sería necesario para que el centro en el que se vaya a desarrollar el intercambio pueda realizar adecuadamente su función educativa, teniendo en cuenta que la participación del alumnado en el programa deberá haber contado con la solicitud o autorización de los titulares de la patria potestad o de los padres o tutores legales. La comunicación responderá al adecuado desarrollo de la relación jurídica solicitada por los propios representantes legales del alumnado.

La transmisión deberá limitarse a los datos que resulten necesarios para el adecuado desarrollo de esa acción educativa y para el cuidado del menor que el centro de destino pudiera requerir.

Cuando el centro destinatario de los datos se encuentre en un país fuera de los Estados miembros de la Unión Europea, la comunicación constituye una transferencia internacional de datos. En este caso el centro deberá consultar previamente con la Delegación de Protección de Datos de la Consejería.

Comunicación de datos a la Administración educativa

Los centros educativos comunicarán los datos personales del alumnado necesarios para el ejercicio de las competencias que tienen atribuidas las administraciones educativas.

Comunicación de datos a otras Administraciones públicas distintas de la autonómica

Cuando lo requiera una ley o por acuerdo entre dichas Administraciones, podrán cederse datos para el ejercicio de sus propias competencias a entidades como Ayuntamientos, Ministerios competentes en materia de educación, de asuntos sociales, de hacienda o bien a distintas instituciones de la Unión Europea.

Comunicación de datos a las fuerzas y cuerpos de seguridad

Las comunicaciones de datos a las fuerzas y cuerpos de seguridad son obligatorias siempre que tengan por objeto la de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

De acuerdo con el RGPD, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la ley. Sin embargo, el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Las fuerzas y cuerpos de seguridad del Estado pueden, en determinadas circunstancias, solicitar datos personales relativos a alumnos matriculados en centros públicos de la Comunidad de Madrid, cuyo responsable último es la Consejería de Educación, Universidades, Ciencia y Portavocía, como por ejemplo la confirmación de su situación de escolarización en un determinado centro educativo.

Conforme al artículo 2 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, , el ámbito de aplicación de esta ley es el tratamiento datos personales realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

El artículo 4 de esta ley establece que las Fuerzas y Cuerpos de Seguridad son autoridades competentes para el tratamiento de datos con los referidos fines. Pero el RGPD establece que no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación

concreta y que "El presente Reglamento no se aplica al tratamiento de datos personales… d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."

Por todo ello, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Salvo que se trate de una emergencia, la forma habitual de requerir información por las Fuerzas y Cuerpos de Seguridad del Estado o por la Policía Local, será el Registro Electrónico, al que deberá remitirse cualquier solicitud que no se presente por este medio, invocando el artículo 155 de la Ley 40/2015, de 1 de octubre del Sector Público.

La solicitud debe incluir la motivación y la finalidad de los datos solicitados, y debe referirse a personas concretas (es decir, no referidas a colectivos o a personas indeterminadas). Además, la información estará referida únicamente a datos identificativos o que permitan la identificación, pero no se facilitará otro tipo de datos que puedan obtenerse de las fuentes de procedencia, como datos de salud, de carácter social o económicos.

Sin embargo, salvo que los datos deban obtenerse con urgencia o emergencia, la solicitud de información sobre alumnos y familiares realizada por las Fuerzas y Cuerpos de Seguridad del Estado o la Policía Local deberá cumplir los siguientes requisitos:

1) Cuando entre en el Registro de la Consejería una solicitud de información, este la remitirá directamente a la Dirección General de Infraestructuras y Servicios, que comprobará si es posible ofrecer toda la información solicitada y contestará directamente por el Registro Electrónico al órgano que la solicita, indicando los datos identificativos del alumno o de sus tutores legales.

2) Si no consta en el sistema toda la información requerida, se derivará la gestión bien al centro educativo para que la comunique por el Registro Electrónico a las Fuerzas y Cuerpos de Seguridad, bien a la DAT correspondiente, que instará al centro para que, si procede, la incorpore en el sistema o la comunique a la DAT, de modo que esta pueda informar a la autoridad que la ha solicitado.

3) Excepcionalmente y por motivos plenamente justificados que impidan el uso del Registro Electrónico, podrá utilizarse el correo electrónico. Tanto en el caso de que se envíe por registro como por correo, el texto del asunto o asiento no deberá incluir datos personales, indicando que la respuesta a la consulta realizada corresponde al expediente o investigación que figuraba en la petición. **El uso excepcional del correo no exime de la remisión por Registro Electrónico,** de modo que quede constancia oficial de que se ha cumplimentado en fecha y forma.

4) En el correo electrónico los datos personales se incluirán en documento anexo, que **deberá cifrarse**, indicando cómo se proporcionará la clave de descifrado. Se aconseja indicar un teléfono al que el peticionario puede llamar para pedir la clave. Si ello no es posible la clave podrá remitirse a la misma dirección de correo electrónico del peticionario, pero en un mensaje independiente. En el documento Envío de datos personales a terceros y Transporte de documentos de forma segura (técnicas de cifrado) se explica cómo realizar estas acciones en la práctica.

Aunque se cumplan los requisitos para la comunicación de datos a las fuerzas y cuerpos de seguridad, es conveniente que en el centro quede documentada la comunicación de los datos.

Cuando se tenga conocimiento de una posible situación de desprotección de un menor: de maltrato, de riesgo o de posible desamparo, se debe comunicar a la autoridad o a sus agentes más próximos.

También cuando se tenga conocimiento de la falta de asistencia de un menor al centro de forma habitual y sin justificación, durante el periodo lectivo, deberá trasladarse a la autoridad competente.

En estos casos no ha de mediar solicitud de ninguna autoridad o institución.

Véase el informe al respecto de la Delegación de Protección de Datos:

20210817 Recomendaciones Cesión datos menores a la policía

Comunicación de datos a servicios sociales

Se pueden comunicar los datos a los servicios sociales siempre que sea para la determinación o tratamiento de situaciones de evaluación o desamparo competencia de los servicios sociales. La comunicación estaría amparada en el interés superior del menor, recogido en la Ley orgánica de protección jurídica del menor. En estos supuestos no se necesita el consentimiento de los interesados.

La comunicación de los datos a los servicios sociales deberá realizarse mediante Registro electrónico.

Comunicación de datos a centros sanitarios

Se pueden facilitar los datos sin consentimiento de los interesados a los centros sanitarios cuando el motivo sea la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que se realicen por profesionales sanitarios sujetos al secreto profesional o por otras personas sujetas a la misma obligación.

El centro educativo podrá solicitar información sobre la asistencia sanitaria prestada en caso de que fuera necesaria para responder de las lesiones causadas como consecuencia del normal desarrollo de la actividad escolar.

Comunicación de datos a Servicios Sanitarios autonómicos o ayuntamientos para campañas de salud o vacunación.

En estos casos, los centros suelen actuar como intermediarios entre los servicios de salud y las familias, por lo que habrán de trasladar a las familias la información de la cual dispongan para que sean ellas las que presten el consentimiento o faciliten los datos a dichos servicios.

No obstante, se pueden facilitar los datos del alumnado a los servicios de salud que los requieran sin necesidad de disponer del consentimiento de los interesados en respuesta a una petición de las autoridades sanitarias cuando sean estrictamente necesarios para garantizar la salud pública o si tiene por finalidad la realización de actuaciones de salud pública que tengan encomendadas. Como pudiera ser un caso de infección en un centro educativo, para la realización de estudios que permitan descartar la presencia de la enfermedad en el entorno del centro educativo.

Comunicación de datos a otras entidades externas para el desarrollo de actividades extraescolares

Se pueden comunicar los datos a instituciones, entidades o empresas que van a ser visitadas por el alumnado en una actividad extraescolar, por ejemplo, una exposición, un museo, una fábrica o un club deportivo, pero se debe contar con el consentimiento previo e inequívoco de los interesados o de sus madres, padres o tutores legales, cuando los datos sean comunicados para las finalidades propias del teatro, museo, exposición o de la fábrica, por ejemplo, el control de entrada, de aforos o para sus programaciones futuras.

La información que sobre estos eventos se facilita a las madres, padres o tutores legales para su autorización debe incluir la relativa a la comunicación de datos a estas entidades, así como la propia autorización. La comunicación, en caso de ser autorizada, implicaría la posibilidad del tratamiento de los datos exclusivamente para los fines que se han indicado, al ser esta necesaria para que el alumnado pueda participar en esa actividad.

Comunicación de datos del alumnado y sus familiares a las asociaciones de madres y padres de alumnos (AMPA).

No se pueden comunicar datos del alumnado ni de sus familiares a las AMPA sin el previo consentimiento de los interesados. Las AMPA son responsables del tratamiento de los datos de carácter personal que hayan recabado, debiendo cumplir con la normativa de protección de datos en su tratamiento.

No obstante, en el caso de que las AMPA fueran contratadas para prestar un servicio al centro educativo para el que tuvieran que tratar los datos del alumnado y de sus madres, padres o tutores, sí tendrían acceso a los datos, pero en la condición de encargadas del tratamiento. En este caso el centro educativo deberá haber informado a los alumnos y a sus familias de la correspondiente política de privacidad.

Comunicación de datos del alumnado a profesionales contratados por las familias

Cuando los padres deciden contratar profesionales externos relacionados con su educación o su salud, es necesario distinguir cuándo el centro educativo está obligado a ceder información a terceros y cuándo no.

Las evaluaciones o informes que se generan sobre los alumnos en los centros educativos forman parte del expediente académico del alumno y se realizan para cumplir con la obligación que establece la LOE de ofrecer la calidad de la

educación para todo el alumnado, independientemente de sus condiciones y circunstancias, así como conseguir el pleno desarrollo de la personalidad y de las capacidades de los alumnos.

Para ello, puesto que se tratan datos personales de carácter sensible para determinar las medidas o adaptaciones necesarias en el correcto desarrollo educativo de los alumnos, se aplica la normativa sobre protección de datos.

A veces, cuando una de las Administraciones competentes detecte una necesidad concreta en relación con el desarrollo de un menor, podrá poner en conocimiento de las otras afectadas, cuando sea estrictamente necesario, dicha circunstancia, así como solicitar información adecuada y pertinente para el correcto diagnóstico y establecimiento de las medidas oportunas conducentes a la capacitación de las habilidades que el menor pueda llegar a desenvolver en la medida de sus posibilidades. Pensemos, por ejemplo, en la obligación que tiene un centro educativo de notificar a las autoridades sanitarias el nombre de una persona que tiene síntomas de COVID19 y la obligación que tienen estas, si se produce caso positivo confirmado, de comunicar al centro que debe confinar el aula o a los contactos estrechos de ese caso.

Es decir, las cesiones de datos que se lleven a cabo deben ser obligatorias para el responsable porque lo establece una norma o porque es necesario para poder llevar a cabo su actividad.

Sin embargo, en el caso de que los padres hayan decidido acudir a una entidad pública o privada para tratar a su hijo están en su derecho de proporcionarle la información que ellos consideren necesaria, incluida la que el centro educativo está obligado a proporcionarle a ellos, como son las evaluaciones psicopedagógicas y los informes que contengan las adaptaciones curriculares. Pero el centro no tiene ninguna obligación ni responsabilidad para tratar información confidencial directamente con el gabinete o profesional psicopedagógico con quienes los padres se han vinculado voluntariamente.

En el caso de que el profesional desee conocer aspectos relacionados con la conducta o aprendizaje del alumno, debería hacerlo a través de los padres. Si estos lo consideran necesario, se podría concertar una reunión donde dicho profesional y los tutores legales estén presentes para realizar alguna aclaración sobre los informes, pero el centro no debe trasladarle ninguna documentación. Para poder demostrar que el tercero acude a propuesta de los padres o tutores, el centro puede solicitarles que previamente comuniquen por escrito la asistencia a la reunión del profesional que trata al alumno por cuenta de aquellos. Incluso se puede convenir entre los participantes en la reunión su grabación si lo consideran adecuado.

No se debe proporcionar a los padres información complementaria como notas o borradores de documentos, pero sí están legitimados para conocer la acreditación de quien los elabora y firma.

Estas circunstancias no son de aplicación cuando puede estar en riesgo la salud o la integridad física de los alumnos.

19. Publicación en la web de datos del profesorado, tutores y otros responsables

Una página web muestra la mayoría de sus contenidos en abierto. Por ello, es necesario contar con el consentimiento previo de los afectados, dado que se trata de una comunicación de datos a los que puede acceder cualquier persona de manera indiscriminada y no resulta necesaria para el ejercicio de la función educativa encomendada a los centros.

Si la consulta de la información está restringida al alumnado del centro y a sus padres o tutores legales mediante acceso al contenido protegido por credenciales, se puede publicar en el entorno restringido, si bien se debe informar a los docentes y, en caso de incluir el teléfono o la dirección de correo electrónico para contacto, que sean las corporativas y no las personales que tenga el profesorado en el ámbito educativo.

20. Contratos menores y cláusulas de protección de datos

Las normas sobre educación permiten a los centros educativos de titularidad de la Comunidad de Madrid, en virtud de su autonomía de gestión económica, contratar con empresas obras, servicios, consultoría y asistencia y suministros por el importe que señale la Ley de contratos del Sector Público para los contratos menores. Todo contrato suscrito con una empresa en los que para proporcionar los servicios contratados sea necesario comunicarle datos personales, deberá incorporar las preceptivas cláusulas de protección de datos. En los contratos menores las cláusulas de protección de datos deberán estar incluidas en la oferta firmada presentada por las empresas oferentes. En la página web de la Delegación de Protección de Datos se ha incorporado una sección llamada “modelos para contratación” con información al respecto (https://dpd.educa2.madrid.org/modelos)

Cuando el objeto principal del contrato sea el tratamiento de datos personales, el contrato será de “encargo de tratamiento” y deberá incorporar toda la información que requiere el artículo 28 del RGPD.

En el caso de que el tratamiento incorpore datos de categoría especial y/o de menores, es necesario realizar una evaluación de impacto. El contrato debe incluir las medidas

técnicas y organizativas de seguridad y privacidad que se deduzcan de dicha evaluación.

Asimismo, el centro educativo debe requerir a la empresa una declaración responsable en la que certifique que sus trabajadores están exentos de antecedentes por delitos sexuales y el compromiso de confidencialidad y deber de secreto del trabajador (necesario si el trabajador va a tener acceso a datos personales).

Véase la nueva guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto. Esta entrada incluye una herramienta para facilitar la evaluación y un vídeo de la presentación de la guía y la herramienta.

21. Videovigilancia

La implantación de cámaras de videovigilancia que responda al interés legítimo de los centros y de la Consejería en mantener la seguridad e integridad de personas y las instalaciones ha de observar la normativa de protección de datos personales, en la medida que implica el tratamiento de los datos de alumnos, profesores, familiares, etc.

Dado el carácter intrusivo de estos sistemas en la intimidad de las personas, su instalación debe responder a los criterios de necesidad, idoneidad para los fines pretendidos, que no se puedan conseguir con una medida menos invasiva de la intimidad, y proporcionalidad, que ofrezca más beneficios que perjuicios. Por ejemplo, cuando el motivo para la instalación de estos sistemas sea el de evitar daños materiales, robos y hurtos que se pueden llegar a producir se podría limitar su funcionamiento a las horas no lectivas, de manera que se minimizara el impacto en la privacidad de las personas.

La intromisión que supone en la intimidad de las personas, tanto del alumnado como del profesorado y demás personas cuya imagen puede ser captada por las cámaras, determina que los sistemas de videovigilancia no podrán instalarse en aseos, vestuarios o zonas de descanso de personal docente o de otros trabajadores.

La instalación de cámaras de videovigilancia en las aulas por motivos de conflictividad resultaría desproporcionada, pues durante las clases ya está presente un profesor o profesora. Además de un control laboral del profesorado, aunque legítimo si este es informado, podría suponer una intromisión excesiva en la privacidad del alumnado.

Cabría la posibilidad de que, fuera del horario lectivo y en los supuestos de desocupación de las aulas, se pudieran activar mecanismos de videovigilancia con la finalidad de protección al alumnado y de evitar daños en las instalaciones y materiales.

Se pueden instalar cámaras en los patios de recreo y comedores cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.

El centro debe informar colocando un distintivo en lugar suficientemente visible en aquellos espacios donde se hayan instalado las cámaras y se deberá disponer de una cláusula informativa que incluya los extremos exigidos por la normativa.

Cuando un centro precise realizar una instalación de videovigilancia deberá redactar un proyecto que tenga en cuenta estas consideraciones y remitirlo a la Delegación de Protección de Datos, que tras verificar que respeta la privacidad de los interesados lo remitirá a la Dirección General competente en el ámbito educativo que corresponda para su aprobación.

22. Fichaje biométrico

El fichaje mediante huella digital comprende el tratamiento de datos biométricos, definido por el RGPD como "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*"

La legitimación del tratamiento no tiene su origen en el consentimiento previo de los afectados, sino en el artículo 6.1.b) "*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte*", así como en el artículo 9, que establece la prohibición del tratamiento, entre otros, de datos biométricos, con varias excepciones, en nuestro caso, que *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".*

En el ordenamiento español, el artículo 20 del Estatuto de los Trabajadores prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores.

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), que ha entendido legítimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores.

La AEPD considera que este precepto daría cobertura también al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto. Hay que señalar que, en ocasiones, para el cumplimiento de sus obligaciones en relación con los empleados públicos, la Administración ha de realizar tratamientos de determinados datos a los que se refiere el RGPD, en su artículo 9, como "categorías especiales de datos".

Debe tenerse en cuenta lo siguiente:

- El trabajador debe ser informado sobre estos tratamientos.
- Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

  En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos[7].
- Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.
- El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.
- Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.
- Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.
- Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
- Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

Aunque los directores de los centros educativos no contratan a los trabajadores que prestan en ellos sus servicios, son los responsables del control horario de quienes prestan en ellos sus servicios. Por ello, están legitimados para adquirir o contratar un sistema digital para dicho control.

[7] Dictamen 3/2012 del Grupo de Trabajo del art. 29

Dado que el responsable del tratamiento de los datos personales es la Consejería, el centro educativo deberá proceder de manera análoga a la solicitud de instalación de sistemas de videovigilancia.

Es decir, deberá redactar un proyecto que justifique la idoneidad y proporcionalidad de la medida, acompañado de una descripción técnica detallada del sistema adoptado, que debe informar expresamente de que dicho sistema de control de presencia y acceso a sus instalaciones no conlleva en ningún momento un análisis biométrico, sino que se elabora un algoritmo identificativo a raíz de una lectura de varios puntos de la huella personal y que los datos del algoritmo no pueden ser descifrados ni desmontados por ninguna entidad no autorizada, puesto que las exigencias derivadas de la protección de datos en el diseño (art. 25.1 RGPD) y, en especial, del principio de minimización, obligan a escoger aquella tecnología que resulte menos intrusiva desde el punto de vista de la protección de datos[8]

También acompañará la notificación de la implantación de la medida de manera completa, clara, concisa y de la información sobre protección de datos a los trabajadores afectados a la que hace referencia el artículo 13 del RGPD.

Dichos documentos deberán ser remitidos a la Delegación de Protección de Datos, que tras verificar que respeta la privacidad de los interesados lo remitirá a la Dirección General competente en el ámbito educativo que corresponda para su aprobación.

Véase las resoluciones de la AEPD sobre este asunto recaídas en sus Procedimientos Sancionadores PS/00128/2020 y PS/00131/2020 **.**

23. Tratamiento de datos por las AMPA

Las asociaciones de madres y padres de alumnos (AMPA) son entidades con personalidad jurídica propia que forman parte de la comunidad educativa y desempeñan un papel significativo en la vida educativa al participar, entre otras actuaciones, en el Consejo Escolar de los centros públicos.

Para el ejercicio de sus funciones, las AMPA suelen tratar datos de carácter personal, identificativos de los familiares del alumnado y de estos, así como otros tipos de datos como pueden ser los económicos, profesionales, sociales, etc.

Como entidades con personalidad jurídica propia que deciden sobre la finalidad, uso y contenido de los datos personales a recabar de los asociados y de sus hijos, las

[8] Dictamen 36-2018 de la Autoridad Catalana de protección de datos en relación con la consulta formulada por un colegio profesional sobre la utilización de sistemas de control basados en la huella dactilar

AMPA son responsables de su tratamiento, por lo que deben cumplir con las obligaciones de la normativa de protección de datos.

Si los padres, las madres o los tutores son asociados al AMPA, el tratamiento estará amparado por la relación que vincula al AMPA con sus asociados, por lo que no será necesario el consentimiento de los progenitores, a los que en todo caso deberá informárseles acerca del tratamiento.

Si no fueran asociados, debería obtenerse su consentimiento. En este caso los centros educativos pueden facilitar a las AMPA información personal de contacto del alumnado y sus familiares solamente si los centros disponen del consentimiento previo de los alumnos o de sus padres o tutores si son menores.

Los centros podrán recabar el consentimiento de los interesados a estos efectos, a los que habrá que informar de la finalidad de la comunicación de datos.

Las AMPA pueden tratar los datos del alumnado por cuenta del centro educativo solo en aquellos casos en los que las AMPA prestasen un servicio al centro que requiera el tratamiento de dichos datos. En estos casos el AMPA actúa como un encargado del tratamiento y requiere la existencia de un contrato que incluya las garantías adecuadas.

Las AMPA únicamente podrán publicar contenidos relativos a los datos del alumnado o sus familiares en su web o en sus redes sociales si cuentan con su consentimiento, o el de sus padres o tutores si son menores, previa información sobre la finalidad de la publicación.

En coherencia con los criterios para la publicación de imágenes de los centros educativos, estas asociaciones deberían seguir esos mismos criterios y evitar la participación en la huella digital del alumnado y sus familiares y no publicar en modo abierto datos que permitan la identificación de las personas, por lo que deberán adoptar los mismos modelos de consentimiento que utiliza el centro al que están adscritas.

24. Guías útiles sobre protección de datos personales

A continuación, incluimos los enlaces a varias guías cuya consulta puede resultar de utilidad en multitud de ocasiones:

AEPD - Guía sobre protección de datos para centros educativos

AEPD - Guía para la notificación de brechas de seguridad

AEPD - Guía y orientaciones para el uso de apps en la nube en el ámbito docente

AEPD - Guía sobre videovigilancia

ADPCat - Buen uso del correo electrónico

Comunidad de Madrid - Instrucciones para el uso del correo electrónico

Madrid Digital – Recomendaciones para el uso de cuentas de correo corporativas

ADPCat - Pautas de protección de datos para centros educativos

IVM - Guía para el tratamiento de datos personales - Víctimas de violencia contra las mujeres

Se autoriza la publicación y difusión del presente documento.

El Director General de Educación Infantil, Primaria y Especial, Firmado digitalmente por: MARTIN BLASCO JOSE IGNACIO Fdo. D. José Ignacio Martín Blasco
El Director General de Educación Secundaria, Formación Profesional y Régimen Especial Firmado digitalmente por: RODRÍGUEZ JIMÉNEZ JOSÉ MARÍA Fdo. D. José María Rodríguez Jiménez
La Directora General de Bilingüismo y Calidad de la Enseñanza Firmado digitalmente por: MARÍN GARCÍA MARÍA MERCEDES Fdo. Dña. Mercedes Marín García
El Director General de Universidades y Enseñanzas Artísticas Superiores Fdo. D. Ricardo Díaz Martín
El Subdirector General de Inspección Educativa Fdo. D. Luis Abad Merino

CONTROL DE VERSIONES

Versión	Cambios	Requiere firma de los responsables
1.0	N/A	SI
1.1	Corrección de errores materiales	NO

NOTA: Cuando una versión del documento requiera firma de los responsables, por incluir nuevas instrucciones o cambios en éstas que sean de su competencia y afecten a la privacidad, se elevará el ordinal de versión mayor (ej. paso de versión 1.5 a 2.0)