PROTECCIÓN DE DATOS

Red de centros SCJ de España

PRESENTACIÓN

La presente guía tiene como objeto ayudar a los centros y a los profesionales de los mismos a ser conscientes de las obligaciones que la ley[1] nos impone con respecto a la protección de los datos personales de las familias, alumnos y personal que en el centro se custodian. Tanto la Titularidad como los Directivos y cualquier tipo de personal contratado queda sujeto a su cumplimiento.

Al final de la guía, como anexos, presentamos dos listas de cotejo:

- Una tiene el objetivo de ayudar a los Equipos Directivos a supervisar el estado del Centro con respecto a la protección de datos;
- La otra es una lista de verificación de los compromisos que la Empresa Consultora, con la que se contraten servicios a este respecto, haya firmado en el contrato.

El Centro

1. Los centros educativos, como responsables de los tratamientos de datos personales que realizan, deben adoptar una serie de medidas de seguridad, de carácter técnico y organizativo, que garanticen la seguridad de los citados datos, es decir, su integridad y confidencialidad y la protección frente al tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

2. Todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre los mismos.

3. Como regla general, los datos personales se conservarán por el tiempo estrictamente necesario para las finalidades para las que se recabaron y para hacer frente a las responsabilidades que se pudieran derivar de su tratamiento, de manera que cuando hayan dejado de ser necesarios o pertinentes para dicha finalidad deberá producirse la cancelación de los mismos.

a. Los datos incluidos en los procesos de admisión serán cancelados una vez finalizados los procedimientos administrativos y judiciales de reclamación.

[1] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD).

b. Los exámenes de los alumnos no deberían mantenerse más allá de la finalización del periodo de reclamaciones.
c. Los datos del expediente académico, en cambio, deben ser conservados, ya que pueden ser solicitados por los alumnos con posterioridad a la finalización de sus estudios.

Consentimiento

4. El consentimiento, cuando es la causa que legitima el tratamiento, se ha de obtener con carácter previo a su recogida. Se puede incluir en el mismo impreso o formulario en el que se recaban los datos.

5. El consentimiento ha de ser por escrito, inequívoco y específico, correspondiendo al centro acreditar su existencia.

6. Bastaría con que el consentimiento se preste al comienzo de cada curso, sin que sea necesario recabarlo nuevamente en cada actividad de tratamiento siempre que responda a la misma finalidad**,** por ejemplo, para los eventos que organice el centro y que estén recogidos en la PGA y calendario escolar
7. Para el acceso a la información contenida en dispositivos electrónicos se requiere el consentimiento de los interesados o de sus padres o tutores si se trata de menores de 14 años. No obstante, en situaciones en las que pudiera estar presente el interés público, 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 los interesados.

Comunicaciones

8. Con carácter general, las comunicaciones entre los profesores y los alumnos deben tener lugar dentro del ámbito de la función educativa y no llevarse a cabo a través de aplicaciones de mensajería instantánea. Si fuera preciso establecer canales específicos de comunicación, deberían emplearse los medios y herramientas establecidas por el centro educativo y puestas a disposición de alumnos y profesores (por ejemplo, áreas específicas en la intranet del centro o uso de plataformas) o por medio del correo electrónico.

9. Como cuestión previa, y como sucede en el caso anterior, las comunicaciones entre los profesores y los padres de los alumnos deben llevarse a cabo a través de los medios puestos a disposición de ambos por el centro educativo. Excepcionalmente, y siempre que se contase con el consentimiento de los padres, sería posible la creación de grupos de whatsapp, de los que sólo formarían parte los padres que hubieran consentido a ello. En todo caso, sería preferible que los grupos fueran gestionados por los propios padres (por ejemplo, a través de un delegado) y la incorporación al grupo no dependiera directamente de los profesores.
10. Los profesores no pueden grabar imágenes de los alumnos y difundirlas a través de aplicaciones de mensajería instantánea a los padres.

Listados y calificaciones

11. Para dar a conocer a los alumnos y a sus padres o tutores la distribución de éstos por aulas, se pueden colocar dichas relaciones en los tablones de anuncios o en las entradas de las aulas, durante un tiempo razonable para permitir el conocimiento por todos los interesados.

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

13. No se pueden hacer públicas las calificaciones de los alumnos. No se recomienda comunicarlas oralmente en clase. No obstante, sí sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, mostrando su calificación frente a la media de sus compañeros.

14. La solicitud por parte de los padres de los exámenes de sus hijos para llevárselos a casa no está sujeta a la protección de datos, sino a la normativa relacionada con el acceso a la documentación y, en su caso, deberá ser resuelta por el centro con arreglo a su normativa interna y demás legislación sectorial que sea de aplicación.

Cesión de datos

15. Se debe contar con el consentimiento previo e inequívoco de los interesados o de sus padres o tutores para comunicar los datos personales de los alumnos a instituciones que van a ser visitadas en actividades extraescolares.

16. No se pueden comunicar los datos de los alumnos y de sus padres a las AMPA sin su consentimiento, a no ser en el caso de que las AMPA fueran contratadas para prestar un servicio al centro educativo.

Imágenes

17. Los centros educativos están legitimados para captar imágenes de sus alumnos durante las actividades escolares como parte de su función educativa. Sí se precisa del consentimiento expreso si se utilizan para la difusión y publicidad del centro o sus actividades.

18. También sería posible la toma de imágenes de los alumnos en determinados eventos desarrollados en el entorno escolar para la única finalidad de que los padres pudieran tener acceso a ellas Este acceso a las imágenes debería siempre llevarse a cabo en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a las imágenes correspondientes a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso recordar a quienes acceden a las imágenes que no pueden, a su vez, proceder a su divulgación de forma abierta.

19. Los profesores, en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados, pueden disponer la realización de ejercicios que impliquen la grabación de imágenes, normalmente de los propios alumnos, que sólo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente. En ningún caso se pueden difundir de forma abierta por internet, redes sociales, etc.

20. Los familiares de los alumnos pueden grabar imágenes en los eventos en los que participan sus hijos siempre y cuando se trate de imágenes captadas exclusivamente para su uso personal y doméstico. Si las imágenes captadas por los familiares se difundieran fuera del ámbito privado, familiar y de amistad, los familiares asumirían la responsabilidad por la comunicación de las imágenes a terceros que no podrían realizar salvo que hubieran obtenido el consentimiento previo de los interesados.

21. Si unos padres se niegan a que se tomen imágenes de sus hijos en un evento escolar, se les ha de informar que la toma de fotografías y vídeos es posible como actividad familiar, exclusivamente para uso personal y doméstico, que está excluida de la aplicación de la normativa de protección de datos.

22. La grabación de imágenes fuera del recinto escolar por los centros requiere el consentimiento de los interesados, o de sus padres o tutores, siempre que no se realice en ejercicio de la función educativa.

23. Si la grabación se realiza por terceros, será obligación de estos terceros disponer del consentimiento de los interesados que habrán podido recabar a través del centro.

Internet y redes sociales

24. La difusión de imágenes de los alumnos por internet requiere el consentimiento de los alumnos o de sus padres o representantes legales.

25. La publicación de datos de profesores y tutores en la web del centro precisa de su consentimiento y se recomienda el uso de direcciones de correo electrónico institucionales.

26. En el uso de plataformas educativas, blogs de profesores, publicación de experiencias educativas, etc. se debe asegurar que los datos de carácter personal publicados no permitan identificar a los alumnos.

27. La publicación de datos personales en redes sociales por parte de los centros educativos requiere contar con el consentimiento inequívoco de los interesados, a los que habrá que informar previamente de manera clara de los datos que se van a publicar, en qué redes sociales, con qué finalidad, quién puede acceder a los datos, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

LISTA DE COTEJO PARA EL CENTRO

Además del cumplimiento de las normas arriba citadas, el Centro debe cumplir los requisitos técnicos de legitimación, identificación del responsable del tratamiento, tratamiento, etc. Al ser una cuestión compleja, facilitamos aquí una lista de cotejo que puede ayudar a revisar periódicamente que todo está en orden. Aún así, es obligación del DPO contratado el revisar estas cuestiones todos los años.

N	Compromisos	Sí/No	Observaciones
RESPONSABLES			
1.	El centro tiene asignado un **responsable de Protección de Datos** que está en contacto con el DPO externo.		
2.	El responsable ha recibido la formación adecuada para el ejercicio de sus funciones.		
3.	El centro tiene asignado un **DPO externo** y conoce sus responsabilidades		
4.	El Centro tiene nombrado un responsable de seguridad informática		
5.	El responsable de seguridad notifica de cualquier incidencia al DPO y éste a la Agencia de protección de datos		
6.	Hay un listado de incidencias posibles con obligación de notificación		
7.	Los usuarios están informados de la obligación de informar siempre que se de una incidencia o brecha en la seguridad (acceso no autorizado, distribución accidental de datos, pérdida de datos…)		
8.	La dirección supervisará que el DPO realice una auditoría de la seguridad del centro, al menos cada dos años.		
9.	Se realizan copias de seguridad y de respaldo de todos los datos.		
10.	Estas copias se custodian bajo llave en un lugar distinto al de los datos y cumplen todas las normas de seguridad (acceso, contraseña, etc.)		

11.	El responsable de seguridad revisa cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de copia de respaldo y recuperación de datos.		

TRATAMIENTO LEGAL

		Reserva	Matrícula	Facturaas	Contratos	Idiomas/interca.	Cert. delitos	Excursiones.	AA.AA.	Servic.Y Extraescol.	Videovigilancia	Emails	Página Web	Cookies	Cart. Currículum
12.	Están debidamente especificadas las cláusulas de:														
	Responsable del fichero														
	Finalidad														
	Legitimación														
	Cesión a terceros														
	Consentimiento														
	Derechos de acceso, rectificación, supresión y oposición…														
	Información adicional														

MEDIDAS DE SEGURIDAD

13.	El documento Medidas de Seguridad existe y ha sido elaborado por la consultora y está actualizado		
14.	Se ha redactado la **relación de usuarios y perfiles de usuario** autorizados donde se establecen las operaciones autorizadas por usuario o perfil.		
15.	Se ha redactado una **circular con las medidas básicas** de seguridad, se ha entregado a los usuarios y la han firmado.		
16.	Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados están en un área de acceso restringido, protegidos con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.		
17.	Los documentos que contengan datos personales se procede a una trituración mecánica para su destrucción (incluidos los exámenes)		
18.	El responsable de seguridad se encarga de dar de baja, de alta y modificar permisos según la normativa y las directrices del Director General del Centro.		
19.	Existe un inventario de equipos, soportes y archivos, debidamente etiquetado e inteligible.		

20.	Existe un procedimiento de actuación ante una brecha en la seguridad.		
21.	Existe un registro de actividades de tratamiento actualizado y revisado por el DPO		
22.	Existe un aviso legal en la página web del colegio informando de las condiciones legales del sitio		
DERECHOS DE LOS TITULARES			
	Se ha redactado un manual de ejercicio de derechos en el que se especifique a los titulares de los datos cómo ejercer sus derechos.		
CONSENTIMIENTOS (En cada caso se estudiará si es oportuno que estos consentimientos estén en la matrícula o en autorizaciones específicas para cada caso).			
23.	Existe autorización para la dispensación de medicamentos		
24.	Existe autorización para la salida del centro de los alumnos durante el recreo y otras salidas excepcionales.		
25.	Existe clausula de consentimiento de tratamiento de datos en el departamento de orientación.		
26.	Existe clausula de consentimiento para la recogida de menores.		
27.	Existe consentimiento para el uso de la imagen del usuario para publicaciones y propaganda del colegio: (la agenda, web del centro, carteles).		
28.	Existe consentimiento para el uso de la imagen del menor en redes sociales, especificando uso para cada una de las redes.		
29.	Existe consentimiento para abrir cuentas personales de correo y de servicios informáticos (Google, Microsoft 365, etc.)		
30.	Existe consentimiento para el tratamiento de los datos personales en la Plataforma Educativa (Educamos, Alexia, Educa, o cualquier otra).		
TRATAMIENTO DE FICHEROS AUTOMATIZADOS			
31.	Los ficheros temporales son cancelados una vez finalizado el tratamiento (listas de participantes a actividades, equipos, pendientes)		

32.	Los ficheros están cifrados o protegidos con contraseña y usuario		
33.	Se ha asignado a los usuarios un usuario y contraseña personal, intransferible.		
34.	Las contraseñas se cambian periódicamente		
35.	La asignación de contraseñas se hará por correo electrónico con acceso restringido al usuario. La contraseña tendrá validez durante 48 horas, para que el usuario pueda cambiarla.		
36.	Las contraseñas se almacenan de modo ininteligible		
37.	Hay mecanismos para limitar intentos reiterados de acceso no autorizado		
38.	Los terminales se bloquean tras 10 minutos de inactividad		
39.	Se ha redactado una política de BYOD ya sean propiedad del centro o del usuario. (Dispositivos informáticos y de comunicación)		
40.	Los sitios web del colegio tienen automatizado la información y consentimiento sobre la instalación de cookies en un sistema de doble capa.		

LISTA DE COTEJO PARA EL CONTROL DE LA EMPRESA

De cara a llevar al día una cuestión tan compleja como esta, proponemos una lista de cotejo de las obligaciones contraídas con la empresa. Debería revisarse con el DPO externo asignado a cada colegio, cada año.

N	Compromisos	Sí/No	Observaciones
REUNIÓN INICIAL			
1.	Se ha tenido la reunión inicial para designar las personas responsables de cada departamento		
2.	Se ha elaborado la planificación y el calendario de las actuaciones		
DOCUMENTACIÓN			
3.	La empresa ha realizado un Registro de Actividades de Tratamiento. (Documento)[2]		
4.	La empresa ha revisado y, en su caso, redactado las clausulas de recabo de consentimiento. (Documentos)		
5.	Se han incorporado los requisitos y detalles del RGPD en (Documentos)		Datos del DPO / Legitimación / Decisiones automatiz. y perfiles / Transmisión a terceros / Derecho de reclamación
6.	Se ha revisado, redactado y entregado los contratos con terceros adecuados al RGPD (Documentos)		
7.	La empresa revisa y redacta los formularios y procedimientos para ejercer los derechos de		

[2] Donde pone “Documentos” se indica que la Empresa debe entregar documentación sobre ese aspecto.

	acceso, olvido, limitación, oposición y portabilidad de los datos personales. (Documentos)		
8.	La empresa mantiene actualizados los textos legales de los portales web del centro y las redes sociales oficiales del centro.		
9.	La empresa entrega documento con política de privacidad y política de cookies. (Documentos)		
10.	La empresa escribe y entrega el protocolo para comunicación de brechas de seguridad. (Documento)		
ANÁLISIS DEL RIESGO Y MEDIDAS DE SEGURIDAD			
11.	La empresa hace un análisis de los riesgos y elabora un documento con medidas de seguridad. (Documento)		
COORDINACIÓN DEL PERSONAL			
12.	La empresa asesora sobre la elección de los encargados del tratamiento		
13.	La empresa supervisa a los encargados del tratamiento		
FORMACIÓN			
14.	La empresa ha realizado una formación general a los empleados de 2 horas de duración, para concienciar e informar sobre la obligaciones respecto a la protección de datos.		
15.	La empresa ha realizado capacitación a los mandos intermedios.		
16.			
SERVICIO DE SOPORTE			
17.	La empresa se compromete a los tiempos de respuesta máximos siguientes: • 8 horas por 5 días a la semana • Incidencia Nivel 1: 1 hora • Incidencia Nivel 2: 12 horas • Incidencia Nivel 3: 24 horas		
RESPONSABILIDADES DPO EXTERNALIZADO			
18.	Supervisa el cumplimiento de lo dispuesto en el RGPD		
19.	Informa y asesora periódicamente al responsable o encargado del tratamiento de sus obligaciones.		

20.	Asesora sobre la Evaluación de Impacto y supervisa su aplicación.		
21.	Analiza de los riesgos asociados a las operaciones de tratamiento.		
22.	Atiende a los interesados en el ejercicio de sus derechos contestando cualquier reclamación de los usuarios.		
23.	Se encarga de la relación y comunicación con la Agencia Española de Protección de datos.		
24.	Existe un registro de actividades de tratamiento actualizado y revisado por el DPO		