COMPRENSION DEL NUEVO MARCO NORMATIVO Y ADAPTACIÓN A LOS CENTROS EDUCATIVOS

CECEGALICIA
FEDERACIÓN AUTONÓMICA DE CENTROS DE ENSINO PRIVADO

RGPD 2016/679

Reglamento UE 2016/679

- Regula el tratamiento de datos personales y la libre circulación de datos en el ámbito de la Unión Europea.
- Pretende a nivel Europeo: unificar la normativa sobre protección de datos y adecuar la misma a la realidad existente.
- Otorga mayor control a los ciudadanos sobre sus datos.
- Aplicación 25 de mayo de 2018.

NOVEDADES RGPD

- Principio de responsabilidad proactiva (acconuntability).
- Delegado de protección de datos para determinadas actividades (DPO). ENSEÑANZA
- Enfoque basado en el riesgo.
- Evaluación de Impacto (PIA).
- Aumentan los derechos de interesados.
- El consentimiento debe ser inequívoco y para categorías especiales de datos expreso.
- Legitimación de tratamiento para cada finalidad.
- Notificar violaciones de seguridad.

Principio de responsabilidad proactiva

- El Responsable del Tratamiento debe aplicar medidas técnicas y organizativas para garantizar el cumplimiento de la normativa de protección de datos y lo debe poder demostrar ante los interesados o la autoridad de control.
- RAT (registro actividades de tratamiento), Análisis de riesgos. Evaluación de Impacto. DPO. Protocolos.

DELEGADO DE PROTECCIÓN DATOS

- Supervisor del cumplimiento RGPD y otra normativa
- Formación, concienciación, auditorías, PIA, asesoramiento, intermediario entre AC, RT e interesados.
- Perfil: conocedor derecho y PD.
- Obligatorio: tratamientos gran escala de datos, autoridades públicas y otras que establezcan estados. EDUCACION.

Enfoque basado en el riesgo.

- Los tratamientos de datos personales que se realizan deben ir acompañados de las medidas necesarias para reducir el riesgo para los derechos y libertades de las personas físicas.
  - Privacidad desde el diseño.
  - Privacidad por defecto.
  - Análisis de riesgos.
  - Evaluación de Impacto.

ANÁLISIS BÁSICO DE RIESGOS

- Herramienta para el análisis de riesgos en actividades de baja exposición a riesgo.
- Se describen y analizan las operaciones de actividades de tratamiento que se agrupan por procesos comunes: se describen las actividades de tratamiento; la tipología de datos, los intervinientes y las tecnologías.
- Se gestiona el riesgo por defecto:
  - Se identifican los riesgos más importantes, que se evalúan por la probabilidad y el impacto.
  - Se establecen medidas de control para reducir el riesgo.
- Supervisión.

EVALUACION DE IMPACTO (PIA)

- Herramienta para evaluar los potenciales riesgos en función de la actividad de tratamiento. Obligatorio cuando existe un riesgo alto para los derechos y libertades o lo establece normativa.
- Describe y analiza: tipos de datos, finalidad, tipos de operaciones de tratamiento, colectivos afectados.
- Se identifica el origen de los riesgos
- Evalúa el riesgo: la probabilidad y el impacto su materialización.
- Trata el riesgo: respuesta para minimizarlos.
- Plan de acción y conclusiones: Se documenta el resultado obtenido junto con el plan de acción que debe incluir las medidas a implantar.
- Supervisión y revisión: mejora continua.

EJEMPLOS DE TRATAMIENTO DE DATOS

- **Actividades de tratamiento**: Solicitud de plaza, Matriculación; Expediente académico; Orientación; Actividades Extraescolares; Servicio de comedor; Personal docente; Personal no docente; Facturación; Videovigilancia…(Ver ficheros inscritos).
- **Operaciones de tratamiento:**. Se pueden agrupar en; captura de datos; clasificación/ almacenamiento; uso/tratamiento; Cesión/ Transferencias; destrucción.

RECOMENDACIONES

- Designar DPO y comunicarlo a AEPD.
- Llevar RAT: descripción de actividad, finalidad, categoría datos, interesados, cesiones y transferencias, períodos de conservación, medidas de seguridad.
- Realizar Análisis de riesgos.
- Justificar o no la necesidad de PIA, y en su caso hacerla.
- Cumplir el deber de información.
- Establecer protocolos de actuación (entrevistas padres, solicitudes de información, almacenamiento en la nube, cesiones de datos, etc).
- Documentar en contrato el acceso a datos del encargado tratamiento.

CUESTIONES PRÁCTICAS

- Consentimiento y legitimidad del tratamiento.
- Deber de Informar
- Minimización de datos y limitación de la finalidad.
- Cesión y Transferencias Internacionales de Datos
- Nube
- Grupos de WhatsApp
- Imágenes

Consentimiento y legitimidad del tratamiento.

- Los colegios en el ámbito de la **función docente y orientadora** están legitimados por ley (también por relación contractual) para tratar datos de alumnos y sus padres, incluidos datos de categoría especial alumnos (religión, salud, etc).
- La legitimación del tratamiento de datos para las actividades extraescolares, y servicios complementarios es la relación contractual.
- Para utilizar los datos para otro fin diferente (ofrecer servicios) debe solicitar consentimiento de forma inequívoca.
- La legitimación del tratamiento de datos de categoría especial basada en el consentimiento debe estar por escrito.
- Los menores pueden prestar consentimiento a partir de los 14 años (incluido).

Deber de informar 1

- Al recabar los datos de los interesados se debe informar sobre; RT, DPO, fines del tratamiento y base jurídica, destinatarios de datos, intención de realizar transferencias internacionales de datos y garantías, plazo de conservación de datos o criterios de determinación, derechos ARCO+POL, derecho a reclamar AC, si la comunicación de datos personales es requisito legal o contractual y consecuencias, si existen decisiones automatizadas.
- Se recomienda añadir en los formularios y contratos la información.
- Información clara y transparente.

Deber de informar 2

- Cuando los datos no se hayan recabado de los interesados se les debe informar en el plazo de un mes (o en la primera comunicación con interesado o antes de comunicar datos a destinatarios), sobre; RT, DPO, fines del tratamiento y base jurídica, categorías de datos, destinatarios de datos, intención de realizar transferencias internacionales de datos y garantías, plazo de conservación de datos o criterios de determinación, derechos ARCOPOL, derecho a reclamar AC, fuente de procedencia de los datos, si existen decisiones automatizadas.

Minimización de datos y limitación de la finalidad.

- Solamente se deben recoger los datos necesarios en relación con la finalidad del tratamiento.
- El personal debe tener únicamente acceso a los datos que necesita según su función.
- Solo se pueden utilizar los datos según la finalidad prevista. Para realizar otro tratamiento se debe informar previamente al interesado. Si el tratamiento está basado en el consentimiento se debe solicitar previamente.

Cesión y Transferencias Internacionales de datos 1

- Hay que informar de las cesiones de datos, y si es preciso obtener autorización. Se debe informar que los datos se cederán a la Consellería, al servicio de catering, a la empresa que presta servicio de autobús, etc. Se debe solicitar consentimiento para ceder los datos al ANPA.
- Hay que informar de las transferencias internacionales de datos (comunicaciones de datos fuera territorio EEE), y en determinados casos se precisa autorización de AC. Se recomienda solicitar el consentimiento explícito para las transferencias internacionales de datos, informando sobre el nivel de garantía del territorio.

Transferencias internacionales de datos 2

- Territorios con nivel adecuado de garantía que no precisan autorización de la AC: Andorra, Argentina, sector privado de Canadá, Suiza, islas Feore, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Uruguay. USA solo entidades certificadas, consultar en https://www.privacyshield.gov

LA NUBE

- Si los datos se alojan en la nube, se debe comprobar en que lugar del mundo se encuentra el servidor. Su está fuera de EEE, se considera Transferencias Internacionales de Datos.
- Almacenamiento en Dropbox, Google Drive, redes sociales, e-mail distinto al servidor del colegio,…Se debe establecer un procedimiento que evalúe la seguridad de la información tratada. El docente debe solicitar previa autorización al centro para su uso. Se recomienda evitar estos sistemas y que prime la plataforma del centro.

Grupos de WhatsApp

- No crear grupos de WhtastApp entre profesores y alumnos. Si fuera necesario por un motivo excepcional es recomendable incluir a algún padre y que éste sea el administrador.
- Grupos de WhatsApp entre padres y profesores. Sólo se deben incluir aquellos padres que hubieran consentido de manera inequívoca. Recomendación que sea administrador algún padre, no el profesor.
- No se puede hacer fotos a los alumnos para enviarlas por mensajería a los padres, salvo casos de fuerza mayor (enfermedad, accidente,..)

Imágenes

- No se precisa el consentimiento de padres o interesados (si tienen 14 años o más), para captar imágenes con fines educativos (trabajo, evaluación).
- Se precisa el consentimiento de padres o interesados (si tienen 14 años o más), si la captación de imágenes no tienen fines educativos.
- La captación de imágenes por asistentes a eventos está permitida si tiene fines domésticos o personales. No deben publicar en internet las imágenes sin autorización de los interesados o representantes.

MUCHAS GRACIAS

CECEGALICIA
FEDERACIÓN AUTONÓMICA DE CENTROS DE ENSINO PRIVADO

RODRÍGUEZ & VILAS
ABOGADOS