Traducido del francés al español - www.onlinedoctranslator.com

GUIAR A SENSIBILIZACIÓN AL RGPD

PARA ASOCIACIONES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil .fr

TABLE DES MATIÈRES

2 PREFACIO

3 INTRODUCCIÓN

3 ¿Cuáles son las obligaciones de las asociaciones en materia de protección de datos?
4 ¿Cuáles son las misiones de la CNIL?

5 LOS CONCEPTOS DE PROTECCIÓN DE DATOS

5 ¿Qué son los datos personales?
5 ¿Qué es el tratamiento de datos personales?
6 ¿Qué es una finalidad?
6 ¿Qué son los datos sensibles? ¿Qué
7 es un controlador de datos? ¿Qué es
7 un destinatario?
8 ¿Qué es un tercero autorizado?
8 ¿Qué es un subcontratista?

9 LOS PRINCIPIOS PRINCIPALES QUE DEBEN RESPETARSE

9 Principio de legalidad
9 Principio de finalidad determinada y legítima
10 Principio de relevancia y minimización
10 Principio de transparencia y respeto de los derechos de las personas
11 Principio de un período de retención limitado
12 Principio de confidencialidad y seguridad
12 Garantizar la seguridad de los datos
12 Garantizar la confidencialidad de los datos

14 LOS PRIMEROS PASOS EN CUMPLIMIENTO

14 1. Enumere los tratamientos
15 2. Ordenar los datos
15 3. Sea transparente
15 4. Organizar y facilitar el ejercicio de los derechos humanos.
dieciséis 5. Asegure los datos

19 PREGUNTAS FRECUENTES

PREFACIO

Francia tiene un tejido asociativo particularmente rico, enumerando más de **1,3 millones de asociaciones** con perfiles diversos tanto por tamaño como por sectores de actividad (benéfico, político, deportivo, social, etc.).

Concentradas en sus misiones, algunas estructuras no siempre cuentan con recursos específicamente dedicados a la protección de datos. Sin embargo, la mayoría recopila mucha información sobre las personas en el curso de sus actividades.

87%

de los franceses dicen que son más sensibles que en los últimos años a la protección de sus datos personal.[1]

Cualquiera que sea el tamaño de la estructura, los riesgos de invasión de la privacidad de las personas interesadas (usuarios, miembros, beneficiarios, etc.) pueden ser importantes en caso de divulgación de información personal a terceros. Por tanto, es fundamental que estas asociaciones preserven los derechos y libertades de las personas interesadas.

Para ayudar a las estructuras asociativas a cumplir con las reglas, en particular el reglamento general de protección de datos (GDPR), la CNIL ofrece herramientas para implementar de manera concreta, y lo antes posible, los principios de las Tecnologías de la Información y las Libertades.

El cumplimiento de la normativa sobre protección de datos personales es realmente necesario para crear un entorno de confianza para los miembros, voluntarios, usuarios, donantes, testadores pero también empleados.

El objetivo de esta guía es, por tanto, cubrir esta necesidad ayudando a las asociaciones a cumplir la normativa en este ámbito. El comprende :

- una presentación de los principales conceptos a conocer;
- una presentación de los principios fundamentales que deben observarse;
- un plan de acción que presenta las principales etapas de cumplimiento;
- preguntas frecuentes.

El sitio web de la CNIL, que ya contiene numerosos recursos para apoyar a los profesionales, se enriquecerá con archivos de esta guía.

Esta guía no responde a necesidades más específicas y no pretende presentar todas las obligaciones que deben observarse al utilizar los datos.

5 Encuesta IFOP para la CNIL realizada en una muestra de 1.001 personas representativas de la población francesa de 18 y más años, diciembre de 2020.

INTRODUCCIÓN

¿Cuáles son las obligaciones de las asociaciones en materia de protección de datos?

El reglamento general de protección de datos (RGPD), que entró en vigor el 25 de mayo de 2018, incorpora los principios fundamentales ya presentes desde 1978 en la Ley de Protección de Datos.

El texto abandona la lógica basada en declaraciones que se enviarán a la CNIL para favorecer una lógica de rendición de cuentas de los actores que utilizan datos personales: las asociaciones ya no tienen que declarar sus archivos a la CNIL antes de su implementación (con excepciones en el sector salud).

A cambio, las organizaciones deben asegurarse de que sus archivos y servicios digitales cumplan en todo momento con el RGPD. Para ello es necesario mantener actualizada la documentación de las actuaciones realizadas para poder demostrar el cumplimiento de la normativa y en particular:

- inventariar los archivos (procesamiento) y mantener el registro detallando los mismos;
- supervisar la subcontratación del procesamiento;
- garantizar la seguridad de los datos;
- organizar la respuesta a las solicitudes de ejercicio de derechos de las personas cuyos datos personales se tratan;
- informar a la CNIL, o incluso a las personas interesadas, de cualquier violación de la seguridad de los datos personales (por ejemplo, pérdida de documentos o violaciones de la seguridad);
- en determinados casos, realizar análisis de impacto en la privacidad (DPIA) para determinados archivos de riesgo.

ENFOQUE EN EL OFICIAL DE PROTECCIÓN DE DATOS (DPO)

La designación de un referente o un DPD / DPO, responsable de pilotar el proceso de cumplimiento del RGPD no es obligatoria para las asociaciones, salvo en determinados casos (una asociación del sector social y médico-social tendrá que designar a priori un DPO en la medida en que procesa datos sensibles a gran escala). Sin embargo, para consolidar relaciones de confianza con las personas afectadas por su tratamiento y limitar los riesgos legales y de imagen asociados al mal uso de los archivos, las asociaciones tienen todo el interés en establecer dicha función (el DPO puede ser interno, externo o compartido) o encomendar a una persona la tarea de garantizar que la estructura cumple con las normas aplicables.

PARA IR MÁS LEJOS

El Delegado de Protección de Datos (DPO) en cnil.fr

¿Cuáles son las misiones de la CNIL?

La Comisión Nacional de Informática y Libertades (CNIL) es la autoridad francesa de protección de datos. Persigue cuatro misiones principales:

Informar y proteger los derechos

La CNIL responde a las solicitudes de particulares y profesionales. Realiza acciones de comunicación con el público en general y los profesionales, ya sea a través de sus redes, la prensa, su sitio web, su presencia en redes sociales o proporcionando herramientas educativas.

Cualquiera puede dirigirse a la CNIL en caso de dificultad para ejercer sus derechos.

Para acompañar conformidad y aconsejar

Para ayudar a los organismos públicos y privados a cumplir con el RGPD, la CNIL ofrece una completa caja de herramientas adaptada a su tamaño y necesidades. La CNIL vela por la búsqueda de soluciones que les permitan perseguir sus objetivos legítimos respetando estrictamente los derechos y libertades de los ciudadanos.

Anticiparse e innovar

Para detectar y analizar tecnologías o nuevos usos que puedan tener impactos significativos en la privacidad, la CNIL proporciona un monitoreo dedicado. Contribuye al desarrollo de soluciones tecnológicas que protegen la privacidad asesorando a las empresas lo antes posible, en una lógica de *privacidad por diseño*.

Controlar y sanción

El control permite a la CNIL verificar la implementación concreta de la ley. Puede exigir a un actor regularizar su expediente (notificación formal) o imponer sanciones (multa, etc.).

PARA IR MÁS LEJOS

En cnil.fr:
- Las misiones de la CNIL
- Situación y organización de la CNIL.

LOS CONCEPTOS DE PROTECCIÓN DE DATOS

¿Qué son los datos personales?

A **información personal** es cualquier información relacionada con una persona física identificada o identificable.

Se puede identificar a una persona física:

- **directamente** (ex. : apellido y Nombre) ;
- **indirectamente** (ex. : un número de membresía, un número de teléfono o matrícula, el número de seguro social, una dirección postal o de correo electrónico, pero también la voz o la foto de una persona).

ATENCIÓN

La identificación de una persona física se puede lograr cruzando un conjunto de datos.

Ejemplos:

- una encuesta por cuestionario a los miembros de una asociación deportiva puede, incluso cuando no se indiquen el nombre y apellido, contener respuestas que permitan conocer la identidad de las personas cuando se combinan entre sí.
- es probable que la recopilación de información relativa a la edad, el sexo y la práctica de un deporte en un nivel determinado en dicha ciudad revele la identidad de la persona.

Por otro lado, los datos de contacto de asociaciones o empresas (por ejemplo, la asociación "Empresa A" con su dirección postal, el número de teléfono de su centralita y un correo genérico de contacto "") no son datos personales.

companieA@email.fr

¿Qué es un procesamiento (o archivo) de datos personales?

a **procesamiento de datos personales** Es cualquier manipulación o uso de datos personales, incluyendo la recogida, registro, organización, almacenamiento, adaptación, modificación, extracción, consulta, uso, comunicación por transmisión o difusión o cualquier otra forma de suministro, conciliación, etc.
Por tanto, esta noción es muy amplia: **cualquier manejo de datos, incluida una simple consulta**, es un "procesamiento de datos personales".

Ejemplos:

- instalación de un sistema de videovigilancia o protección por video para la seguridad de las personas y los bienes dentro de la asociación;
- una hoja de cálculo (Excel, Calc, etc.) que agrupa todas las acciones realizadas para ayudar a los usuarios;
- el formulario de afiliación a la asociación;
- una base de datos que reúne toda la información relativa a los usuarios;
- etc.

ATENCIÓN

Un archivo o procesamiento de datos personales **no está necesariamente computarizado** : Los archivos en papel también se ven afectados y deben protegerse en las mismas condiciones.

¿Qué es una finalidad?

El tratamiento de datos persigue siempre un objetivo: este es su "propósito". Esto debe ser determinado, explícito y legítimo antes de la recopilación de los datos y su uso. Dicho de otro modo,**No está permitido recopilar datos si no sabemos antes qué uso haremos de ellos.**.

EJEMPLOS

- la gestión administrativa de los titulares de licencias dentro de una asociación deportiva;
- gestión administrativa de donantes dentro de una asociación benéfica;
- apoyo y seguimiento social de personas en dificultad dentro de las asociaciones sociales;
- mantener un directorio de ex miembros de una asociación;
- la realización por cualquier medio de comunicación de operaciones relacionadas con acciones de prospección caritativa / política / comercial con miembros, miembros, donantes, prospectos;
- etc.

Hay que respetar el objetivo: no puedes utilizar tu expediente para ningún otro fin que no sea el que se ha fijado. Por ejemplo, no puede reutilizar el archivo de reclutamiento de solicitudes para un puesto de voluntario y / o empleado para proponer ofertas comerciales / benéficas relacionadas con su asociación a los candidatos.

¿Qué son los datos sensibles?

los **informacion delicada** son las que se refieren al supuesto origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas o afiliación sindical. También incluyen datos genéticos, datos biométricos, datos relacionados con la salud y datos relacionados con la vida sexual u orientación sexual de una persona física.

El uso de estos datos está, en principio, prohibido salvo en los casos límite previstos en el artículo 9.2. del RGPD.

Entre estas excepciones se encuentran:

- el consentimiento explícito del interesado;
- o el hecho de que las siguientes condiciones **reunirse** :

- el archivo está creado por una fundación, una asociación o cualquier otra organización sin fines de lucro;
- la asociación persigue un objetivo político, filosófico, religioso o sindical;

- el expediente se refiere exclusivamente a miembros o ex miembros de este organismo o personas que mantienen contacto regular con él en relación con sus fines;
- estos datos no se comunican fuera de esta organización sin el consentimiento de las personas interesadas.

- o el hecho de que las siguientes condiciones **reunirse** :
  - el archivo está creado por una fundación, una asociación o cualquier otra organización sin fines de lucro;
  - la asociación persigue un objetivo político, filosófico, religioso o sindical;
  - el expediente se refiere exclusivamente a miembros o ex miembros de este organismo o personas que mantienen contacto regular con él en relación con sus fines;
  - estos datos no se comunican fuera de esta organización sin el consentimiento de las personas interesadas.

EJEMPLOS

- una asociación que organice excursiones extracurriculares puede recopilar información relacionada con la salud de los niños (por ejemplo: alergias, etc.) después de obtener el consentimiento del representante legal;
- Un partido político podrá recoger las opiniones políticas de sus miembros o de las personas con las que mantenga contacto regular en relación con sus misiones, siempre que no se comuniquen fuera de este organismo (salvo que el interesado haya dado su consentimiento a esta comunicación).

PARA IR MÁS LEJOS

Datos sensibles (definición) en cnil.fr

¿Qué es un controlador de datos?

La persona u organización que **define los objetivos que persigue un tratamiento y sus métodos prácticos** (información recopilada, por ejemplo) se llama **controlador de datos**.

Es él quien debe asegurarse de que el expediente que implemente respete las reglas.

El controlador de datos generalmente está representado por el representante legal de la estructura.

EJEMPLOS

- el presidente de la organización benéfica;
- el director general de la estructura deportiva;
- etc.

¿Qué es un destinatario?

a **beneficiario** es una persona u organización que recibe datos personales por un motivo específico y legítimo.

EJEMPLOS

- el organizador de un torneo;
- la federación deportiva a la que está adscrito un club;
- profesionales que trabajan en la unidad de recogida de información preocupante (CRIP) del departamento donde reside el menor, si algún miembro de la asociación escribe información preocupante con el fin de comunicar una situación de peligro o riesgo de peligro en la que se encuentra un menor.

¿Qué es un tercero autorizado?

a **tercero autorizado** es una autoridad pública o una administración autorizada por un texto (ley, decreto, etc.) para recibir datos personales.

EJEMPLOS:

- Pôle Emploi o las organizaciones de seguridad social como parte de la lucha contra el fraude;
- las administraciones de justicia, la policía, la gendarmería;
- etc.

PARA IR MÁS LEJOS

La guía de "terceros autorizados" en cnil.fr

¿Qué es un subcontratista?

a **subcontratación**, que es una categoría de destinatarios, es la empresa o asociación que maneja datos en nombre de un controlador de datos como parte de un servicio o servicio.

Un procesador tiene obligaciones con respecto a los datos personales, que deben especificarse en el contrato.

EJEMPLOS

- Proveedores de servicios de TI (alojamiento, mantenimiento, etc.);
- cualquier organización que ofrezca un servicio o un servicio que implique el procesamiento de datos personales en nombre de otra organización (por ejemplo: gestión de nóminas para empleados de asociaciones, etc.).

PARA IR MÁS LEJOS

Trabajar con un subcontratista en cnil.fr

Principio de legalidad

El tratamiento debe ser **legal**. Para hacer esto, debe:

- perseguir un objetivo que no esté en contra de la ley (por ejemplo, el procesamiento de datos no puede tener como objetivo una discriminación ilegal);
- estar basado en una base legal prevista por el RGPD.

Antes de implementar su expediente, debe elegir la base legal entre las probable que sea utilizado por una asociación:

- **acuerdo libre, específico, ilustrado e inequívoco** personas (por ejemplo: prospección electrónica con prospectos, etc.);
- **ejecución del contrato** (ex. : la prestación de los servicios definidos en el marco del contrato celebrado entre la asociación deportiva y el interesado o su representante legal y la gestión administrativa de los interesados);
- **el cumplimiento de una misión de interés público** (para las asociaciones de derecho privado encargadas de una misión de interés público o dotadas de prerrogativas de autoridad pública únicamente);
- **la satisfacción del interés legítimo** la organización (por ejemplo: escrutinio por correo a los miembros, etc.);
- **cumplimiento de una obligación legal** que impone el tratamiento de estos datos (por ejemplo: cuando la asociación realiza la declaración social nominativa para sus empleados).

PARA IR MÁS LEJOS

Bases legales en cnil.fr

Principio de una finalidad determinada y legítima

Los datos deben recopilarse para un **objetivo determinado y legítimo**. Este objetivo inicial perseguido por su organización debe ser respetado: no puede utilizar los datos por un motivo distinto al inicialmente fijado.

EJEMPLO

Un centro musical no puede transmitir los datos de contacto de sus miembros recopilados para la organización de lecciones a una tienda de instrumentos musicales que desee enviar publicidad, si los miembros no han dado su consentimiento previamente.

PARA IR MÁS LEJOS

Definir un propósito en cnil.fr

Principio de relevancia y minimización

Una vez que se ha definido con precisión el propósito del tratamiento, debe **determinar los datos necesarios para lograr este objetivo.**

Estos datos deben:

- tener un vínculo directo con el objeto perseguido;
- Ser necesario para el objetivo perseguido.

En otras palabras, debe limitar la cantidad de datos procesados tanto como sea posible.

EJEMPLO

La información relacionada con el estado civil de una persona no parece ser necesaria en el contexto del registro para una actividad deportiva.

PARA IR MÁS LEJOS

Verificar la relevancia de los datos en cnil.fr

Principio de transparencia y respeto a los derechos humanos

Los miembros deben comprender por qué se recopilan sus datos y qué derechos pueden ejercer. Por tanto, debes**ser transparente tan pronto como se recopilen los datos.**

Los interesados deben conocer las principales características del tratamiento realizado, es decir:

- los'**identidad y datos de contacto de su organización** ;
- los'**propósito del tratamiento** (para qué se utilizarán los datos recopilados, por ejemplo: gestión de partes interesadas, gestión de miembros, elecciones a la junta directiva, etc.);
- los **base legal** (ver “principio de legalidad” pág. 9);
- los'**obligación o no del interesado de proporcionar esta información** así como las consecuencias para la persona en caso de no suministro de datos;
- los **destinatarios o categorías de destinatarios de los datos** (las personas a las que se comunican los datos, ver “los principales conceptos a conocer” p. 7. Por ejemplo: la federación deportiva a la que está afiliado el club);
- los **período de retención de datos** (cuánto tiempo los datos son de interés para su organización. Luego, los datos se eliminan o se anonimizan);
- los **derechos de los interesados** (al menos los derechos de acceso, rectificación, supresión y limitación que son aplicables para todo el procesamiento);
- la existencia o no de un **transferencia de datos**s fuera de la Unión Europea (indicando el país y la herramienta legal utilizada para proteger los datos);

- los **formas de ponerse en contacto con el delegado de protección de datos** la organización o el referente de “protección de datos personales”;
- los **derecho a presentar una denuncia ante la CNIL.**

Esta información debe presentarse de manera concisa y transparente. Deben adaptarse a su público (pictogramas para niños, por ejemplo).

BUENA PRÁCTICA

Para evitar menciones demasiado largas en un formulario, puede indicar la identidad del responsable del tratamiento, el objetivo que persigue el tratamiento y los derechos de las personas al final del formulario haciendo referencia a un aviso de información completo en el sitio web de la Asociación. .

Este esfuerzo de transparencia debería permitir a las personas interesadas**ejercer sus derechos**. Por lo tanto, debe permitirles que lo hagan fácilmente (ver"Organizar y facilitar el ejercicio de los derechos humanos", pag. 15).

Principio de una vida útil limitada

Los datos deben conservarse durante un período de **tiempo limitado** definido según el objetivo perseguido por el tratamiento.

Durante este período, se deben distinguir varias fases:

1. Los datos son necesarios para la gestión diaria de su asociación.
2. Los datos ya no son necesarios a diario, pero aún presentan un **interés administrativo** (por ejemplo, la gestión de un posible litigio) o se debe conservar para dar respuesta a **una obligación legal** (por ejemplo: las nóminas de los empleados de su organización deben conservarse durante cinco años).

Durante la segunda fase, denominada "archivo intermedio", el acceso a los datos debe limitarse aún más para que solo puedan ser consultados de forma ad hoc y por personas cuyas misiones lo justifiquen (por ejemplo, cuando los datos pasan de la "base de datos activa ”A la“ base de datos de archivo intermedio ”, ya no deben estar disponibles para consulta de todas las personas inicialmente previstas, sino únicamente de personas especialmente autorizadas, que tengan interés en conocerlas por sus funciones (por ejemplo, el servicio a cargo de litigio).

Una vez transcurridos estos tiempos, debes:

- **borrar** datos si ya no son de interés para la organización;
- Dónde **anonimizar** datos siempre que los interesados ya no sean identificables en absoluto.

PARA IR MÁS LEJOS

Periodos de conservación de datos en cnil.fr

Principio de confidencialidad y seguridad

Los datos deben ser vistos y procesados por la menor cantidad de personas posible. En la práctica, solo los miembros y empleados de la asociación cuyas misiones así lo requieran deberían poder acceder a los datos procesados por su asociación.
Esto significa que debes **garantizar la seguridad y confidencialidad de los datos** con el fin de limitar la divulgación de datos a personas internas o externas que no necesitan conocerlos.

Garantizar la seguridad de los datos

Para ello, debe tomar medidas para garantizar la seguridad de los locales y puestos de trabajo.

EJEMPLOS

- Cierre de locales, armarios, oficinas;
- Las contraseñas individuales se renuevan con regularidad;
- Elección de un antivirus.

Las medidas de seguridad deben adaptarse a la naturaleza de los datos tratados por su organización y los riesgos que una divulgación podría representar para las personas interesadas (robo de identidad, phishing, chantaje, etc.).

BUENA PRÁCTICA

Al eliminar datos personales en formato "papel", puede desechar los documentos en un contenedor de documentos confidenciales o triturarlos para garantizar su confidencialidad.

PARA IR MÁS LEJOS

El consejo de la CNIL para una buena contraseña en cnil.fr

Garantizar la confidencialidad de los datos

Para no comunicar información a personas no autorizadas, debe estar atento.

En interno, Las autorizaciones de TI deben gestionarse para que no todo el mundo pueda acceder a toda la información.

En caso de solicitud de acceso o comunicación de datos por parte de otro organismo, debe garantizar la legitimidad de la solicitud:

- si es un **autoridad pública o una administración autorizada por un texto para recibir datos personales** (por ejemplo: la CNIL en el marco de su poder de supervisión):

  - consultar el texto que le autoriza a solicitar esta información;
  - analizar la calidad de la organización y el alcance de la información solicitada;
  - comunicar solo la información que debe comunicarse mientras se asegura la transmisión de datos.

- si es una solicitud hecha por un t**iers que no tienen un texto que autorice esta solicitud** :

  - analizar el **legitimidad de la solicitud** velar por que la reutilización prevista por la organización sea compatible con el motivo de la recogida de datos;
  - hacer una **ordenar datos** con el fin de comunicar solo aquellos que son **requerido** el objetivo perseguido por la organización;
  - **Informar a las personas interesadas y permitirles oponerse a esta transmisión.** ;
  - **indicar en su documentación** este nuevo destinatario.

BUENA PRÁCTICA

Al ordenar los datos, su asociación debe analizar el nivel de detalle necesario para la organización solicitante.

En determinadas circunstancias, los datos anonimizados o los datos que no identifican directamente al interesado pueden resultar suficientes (por ejemplo: en el contexto de una solicitud de un organismo público o privado para una subvención o patrocinio, la constitución de un archivo que contenga datos anonimizados la información parece en principio suficiente).

LOS PRIMEROS PASOS EN CUMPLIMIENTO

Tener en cuenta el RGPD no debe verse solo como una restricción técnica o legal. Es sobre todo una oportunidad para hacer balance de los datos tratados y el uso de archivos y servicios digitales en la asociación.

El cumplimiento de las normas de "tecnologías de la información y libertades" es un proceso continuo (formación, desarrollo de procedimientos, etc.) que pasa por varias etapas.

1. Enumere los archivos

El RGPD requiere que se enumeren en un documento específico (el registro) los archivos que ha creado o utiliza.

Este registro proporciona una visión clara y global de las actividades de la asociación que requieren la recopilación y el uso de datos personales.

En su registro, cree un archivo para cada objetivo de archivo, especificando:

- el nombre y los datos de contacto del responsable del tratamiento y, si existen, del responsable conjunto, el representante del responsable y el delegado de protección de datos;
- el (los) objetivo (s) que persigue cada expediente (por ejemplo, la gestión de socios);
- las categorías de interesados y datos utilizados (por ejemplo, nombre, dirección, etc.);
- quién tiene acceso a los datos (es decir, personas autorizadas como, por ejemplo, el departamento de recursos humanos para la nómina) y a quién se comunicarán (los destinatarios, por ejemplo, las autoridades fiscales);
- los períodos de retención de estos datos (vida útil y período de retención de archivos);
- las medidas de seguridad implementadas (por ejemplo: política de contraseñas, etc.);
- si es necesario, transferencias de datos personales fuera de la Unión Europea o a una organización internacional.

ATENCIÓN

El desarrollo del registro requiere estar en contacto regular con miembros, empleados y subcontratistas que puedan manejar datos personales.

PARA IR MÁS LEJOS

El registro de actividades de procesamiento (la CNIL propone un modelo de registro básico) en cnil.fr

2. Ordenar los datos

Cada registro en el registro le permite verificar:

- que los datos tratados son relevantes y necesarios para el objetivo perseguido **(principio de relevancia y minimización)**.

  > Por ejemplo, al dar de alta a un socio para una actividad de ocio o una estancia organizada por la asociación, es legítimo solicitar un certificado del cociente familiar para la aplicación de una tarifa preferencial. Por otro lado, no es relevante solicitar el número de la seguridad social del afiliado o de su representante legal o incluso una copia de su tarjeta Vitale.

- que solo las personas autorizadas tengan acceso a los datos que necesitan y que existan medidas de seguridad adecuadas **(principio de confidencialidad y seguridad)**.

  > Por ejemplo, la información relativa al pago de cotizaciones por parte de los miembros de una asociación deportiva sólo debe ser accesible al personal administrativo encargado de su seguimiento y no a todos los miembros, ni siquiera a todos los miembros encargados de la formación.
  >
  > La asociación debe definir perfiles de autorización separando los derechos según las tareas a realizar por cada uno para limitar el acceso de los usuarios solo a los datos necesarios.

- que los datos no se conserven más de lo necesario **(principio del período de conservación de datos limitado)**.

  > Por ejemplo, la asociación no puede conservar datos sobre sus antiguos miembros / miembros de forma indefinida. Debe eliminarlos tres años después de que finalice la membresía de la persona.

3. Sea transparente

Las personas deben ser informadas cada vez que se recopilen datos personales, en papel o en formato digital (cuestionarios, formularios de afiliación, formularios de suscripción, etc.). Se recomienda la información oral además de la información escrita para asegurar que la persona interesada comprenda la información comunicada.

PARA IR MÁS LEJOS

En cnil.fr:
- Cumplimiento del RGPD: ¿cómo informar a las personas y garantizar la transparencia?
- GDPR: ejemplos de avisos de información

4. Organizar y facilitar el ejercicio de los derechos humanos.

Las personas (miembros, empleados, proveedores de servicios, etc.) tienen derechos sobre sus datos. Cualquiera interesado puede así:

- **obtenga confirmación si está procesando o no** información al respecto, acceder a ella y obtener una copia;

- **rectificar** información inexacta o incompleta sobre él;
- **borra tus datos** (ex. : la persona ha retirado el consentimiento en el que se basa el tratamiento, etc.);
- **solicitar la limitación o "congelación" de datos** (por ejemplo, cuando la persona cuestiona la veracidad de sus datos, puede solicitar a la organización que congele temporalmente el tratamiento de sus datos, mientras realiza las verificaciones necesarias);
- **recuperar sus datos para su reutilización (derecho a la portabilidad)** : este derecho solo se aplica si se cumplen las siguientes tres condiciones: limitación a solo los datos personales proporcionados por el interesado; si los datos se procesan de manera automatizada (exclusión de archivos en papel) sobre la base del consentimiento previo del interesado o la ejecución de un contrato celebrado con el interesado; respetar los derechos y libertades de terceros;
- **oponerse al tratamiento** siempre que se invoquen motivos específicos y si el tratamiento se lleva a cabo sobre la base jurídica del interés legítimo del responsable del tratamiento, o para el desempeño de una misión de interés público o una misión que recaiga en el ejercicio de la autoridad pública (por ejemplo, el responsable del tratamiento puede negar al interesado el ejercicio de su derecho de oposición si el tratamiento de la información que le concierne se basa en una obligación legal).

Debe facilitar a las personas el ejercicio de estos derechos.

BUENA PRÁCTICA

Si tiene un sitio web, planifique un formulario de contacto específico, un número de teléfono o una dirección de correo electrónico dedicada. Si ofrece una cuenta en línea, dé a los miembros la opción de ejercer sus derechos desde su cuenta. Establecer un proceso interno para asegurar la identificación y procesamiento de solicitudes en plazos cortos (un mes como máximo). Si se necesita tiempo adicional para procesar la solicitud (por ejemplo, debido a su complejidad), el interesado debe ser informado dentro del mismo plazo de un mes. En todos los casos, debe proporcionarse una respuesta en un plazo que no podrá exceder de tres meses.

PARA IR MÁS LEJOS

Respeta los derechos de las personas. en cnil.fr

5. Asegure los datos

Los incidentes, internos o externos, malintencionados o accidentales, pueden tener consecuencias importantes para las personas cuyos datos se ven afectados (reputación, chantaje, etc.).

Para limitar los riesgos, debe implementar medidas de seguridad para prevenir:

- acceso ilegítimo a los datos (violación de la confidencialidad);
- su modificación no deseada (daño a la integridad);
- su desaparición (deterioro de la disponibilidad).

Estos riesgos no son teóricos. Todos los días, la CNIL recibe notificaciones de violaciones de datos y quejas por falta de seguridad.

BUENA PRÁCTICA

Los empleados y voluntarios tienen su propio identificador con una contraseña personal y sólida que se actualiza periódicamente y se almacena de forma segura dentro del sistema de información. El acceso remoto a los recursos de la asociación, como el back-office del sitio web que permite la gestión de miembros, se realiza de forma segura en un canal encriptado y autenticado (https).

Su acceso a los archivos se define de acuerdo con sus necesidades reales en relación con el ejercicio de su misión y sus cuentas de TI se cierran al final de su contrato. El pago de las contribuciones se realiza a través de un canal encriptado y autenticado (https). Los armarios están cerrados con llave y el acceso a las instalaciones y servidores, así como los documentos en papel, solo se permite a las personas que lo necesiten.

PARA IR MÁS LEJOS

En cnil.fr:
- Contraseñas: recomendaciones de seguridad mínimas para empresas y particulares
- Asesoramiento de la CNIL para una buena contraseña
- Genere una contraseña segura

A continuación, se muestran algunas comprobaciones que ya puede realizar:

- [ ] ¿El acceso a las instalaciones es seguro? (por ejemplo: alarma, sistema de videovigilancia, etc.)
- [ ] ¿Están los armarios y las cajas fuertes cerradas sistemáticamente?
- [ ] ¿Están las cuentas de usuario protegidas por contraseñas de complejidad suficiente? ¿Se
- [ ] eliminan las cuentas de usuario cuando un usuario se va?
- [ ] ¿Se proporcionan perfiles separados de acuerdo con las necesidades de los usuarios para acceder a los datos?
- [ ] ¿Son seguras las estaciones de trabajo (por ejemplo: bloqueo automático de sesiones, antivirus y software actualizado)?
- [ ] ¿Los miembros de la asociación son conscientes de la protección de la privacidad? ¿Se firma un estatuto de TI?
- [ ] ¿Se utilizan móviles multifunción (smartphones), portátiles o llaves USB? ¿Está regulado su uso?
- [ ] ¿Existen procedimientos regulares de respaldo y recuperación de datos en caso de un incidente?
- [ ] ¿Su sitio web utiliza un protocolo seguro para las páginas en las que se muestran o transmiten datos personales (por ejemplo, autenticación, formulario en línea)?

PARA IR MÁS LEJOS

En cnil.fr:
- Guía de seguridad de datos personales desarrollada por la CNIL
- Todo el contenido de ciberseguridad de la CNIL

El sitio www.cybermalveillance.gouv.fr También ofrece ayuda en línea, así como una lista de proveedores aprobados.

¿Qué hacer en caso de violación de datos?

¿Se han destruido, perdido, modificado o revelado datos personales accidental o ilegalmente (correos electrónicos enviados a destinatarios incorrectos, equipo perdido o robado, publicación involuntaria de datos en Internet, etc.)? Este incidente constituye una "violación de datos".

Cuando ocurre un incidente de este tipo, es necesario documentarlo dentro de la asociación. En caso de inspección, este documento es verificado por los servicios de la CNIL.

Si existe un riesgo para los derechos y libertades de los interesados, **debe informar esta violación a la CNIL dentro de las 72 horas**. Esta notificación se realiza en línea en el sitio web de la CNIL.

Finalmente, si estos riesgos se consideran altos para estas personas, debe informarles.

Para determinar el riesgo para las personas, se debe tener en cuenta al menos lo siguiente:

- el tipo de violación (integridad, disponibilidad, confidencialidad);
- la naturaleza, la sensibilidad y el volumen de los datos personales;
- facilidad de identificación de los interesados;
- la gravedad de las consecuencias para las personas afectadas;
- las características particulares de las personas afectadas (menores, personas vulnerables, soldados, etc.);
- las características particulares del responsable del tratamiento (objeto de la asociación que pueda revelar información personal sensible, por ejemplo);
- el número de personas involucradas.

PARA IR MÁS LEJOS

En cnil.fr:
• Violaciones de datos personales
• Notificar una violación de datos en el sitio web de la CNIL

PREGUNTAS FRECUENTES

¿Pueden los ayuntamientos pedir a las asociaciones que subvencionan que les envíen el expediente de sus afiliados?

No, un municipio no puede solicitar, incluso cuando otorga un subsidio a una asociación, la lista de nombres de sus miembros.

Por otro lado, los ayuntamientos pueden solicitar la **copia certificada del presupuesto y las cuentas del ejercicio anterior**, así como la comunicación de todos los documentos que muestren los resultados de la actividad de la asociación, para controlar el uso de las subvenciones que han pagado.

¿Puede una asociación comunicar información sobre sus miembros a terceros autorizados?

Sí, la comunicación de información sobre socios y empleados a "terceros autorizados" (ver pág. 8) es posible con la condición de que se base en un texto legal (ley, decreto, etc.).

Para cada solicitud, debe asegurarse de que:

- **La solicitud de comunicación es por escrito y se basa en un texto que la autoriza.**. Debe asegurarse de que la solicitud se corresponda con lo permitido por los textos presentados por el solicitante. Si tiene alguna duda, puede preguntar a la CNIL (por ejemplo: una simple solicitud por teléfono sin verificación específica no puede dar lugar a la transmisión de datos);
- **el solicitante está bien citado en el texto y está autorizado** requerir la comunicación de información;
- **la frecuencia y el alcance de la solicitud de comunicación** (naturaleza de los datos, interesados y tipo de tratamiento en particular) **no exceda lo prescrito por la ley** (por ejemplo, respeto por la confidencialidad médica).

Debe asegurarse de que la transmisión de información se lleve a cabo de manera segura (por ejemplo, entrega en mano, uso de cifrado en caso de transmisión por computadora, etc.).

Finalmente, debe mantener registros de la solicitud y la respuesta proporcionada en caso de cualquier litigio (por ejemplo: copia de la solicitud, identificación del agente o departamento solicitante, alcance de los datos transmitidos).

PARA IR MÁS LEJOS

La guía de "terceros autorizados" en cnil.fr

¿Puede un miembro de una asociación exigir la comunicación de la lista de todos los demás miembros?

Sí, pero solo si los estatutos de la asociación prevén esta posibilidad.

Una asociación es libre de especificar en sus estatutos que la membresía implica aceptar que sus datos de contacto puedan ser comunicados a un miembro que lo solicite, con la condición de que esta comunicación tenga un vínculo directo con la actividad de la asociación.

¿Puede una asociación deportiva publicar en línea los resultados deportivos de los titulares de licencias?

Sí, Las estructuras deportivas pueden publicar los resultados deportivos de los licenciatarios en línea sujeto al cumplimiento de ciertas condiciones al recopilar información:

- el interesado ha sido informado de la publicación de sus resultados en línea;
- puede oponerse a esta publicación de forma sencilla (por ejemplo: una casilla de verificación puesta a su disposición en el formulario de participación en una competición deportiva), señalando una situación concreta que la justifique.

¿Puede una asociación publicar fotos de sus miembros en su sitio web o dentro de su revista?

Sí, siempre que la persona fotografiada (y el tutor legal de un menor) hayan dado su consentimiento para esta distribución.

Asimismo, las personas interesadas deberán autorizar la captura y uso de su imagen por motivos concretos, preferiblemente por escrito y enviársela para que usted pueda distribuir la fotografía.

ATENCIÓN

La publicación de fotografías de menores debe ser objeto de especial vigilancia.

¿Puede una asociación utilizar los datos de sus miembros para realizar campañas de recuperación de membresía cada año?

Sí, una asociación puede utilizar los datos de sus miembros para llevar a cabo campañas de recuperación de membresía cada año bajo ciertas condiciones.

La CNIL recomienda que la información relativa a un miembro se mantenga durante un período de tres años a partir de la finalización de su membresía. Durante este período, y durante cada solicitud, la persona interesada debe poder oponerse al uso de sus datos de contacto para recordatorios de membresía de una manera simple y gratuita (por ejemplo, un enlace para darse de baja al final de cada correo electrónico).

Una vez transcurrido el plazo de tres años, la asociación deberá ponerse en contacto con el interesado para saber si desea seguir recibiendo prospección comercial por su parte. De lo contrario, o sin una respuesta suya, el interesado ya no debería recibir ninguna solicitud de la asociación y sus datos serán eliminados o archivados.

¿Puede una asociación recopilar los antecedentes penales de sus empleados / voluntarios?

No, Las asociaciones no pueden recopilar un extracto de los antecedentes penales de sus empleados y / o voluntarios.

Los organismos de derecho privado no pueden procesar datos relacionados con infracciones, con algunas excepciones. Se trata de una prohibición en principio que no renuncia al consentimiento del interesado.

Al unirse a la asociación, ¿cómo informar a los futuros miembros / miembros del tratamiento de sus datos?

Debe ser transparente con respecto a los interesados especificando las características del tratamiento (las finalidades del tratamiento, los plazos de conservación, los destinatarios, los derechos que tienen, etc.) al recoger su información.

La información puede ser entregada a la persona y su representante legal por cualquier medio (ej .: avisos informativos insertados en el formulario de membresía de su estructura o en el cuadernillo de presentación de éste, en la parte inferior de los formularios de contacto, etc.) y debe ser adaptado al público (por ejemplo: se pueden favorecer las imágenes lúdicas cuando se trata de niños, orales, pictogramas, etc.).

Se recomienda recurrir a información oral además de información escrita para asegurar la correcta comprensión de la información comunicada.

PARA IR MÁS LEJOS

En cnil.fr:
- Los avisos de información enumerados en el artículo 13 del RGPD
- Cumplimiento del RGPD: ¿cómo informar a las personas y garantizar la transparencia?
- Ejemplos de menciones de información.

¿Puede una asociación comunicar por correo / correo electrónico / SMS información relacionada con las actividades de su asociación (próximos eventos, boletín informativo, etc.) a sus miembros / miembros?

Sí, la asociación puede comunicarse con sus miembros / miembros a través de correo electrónico / correo / sms siempre que las personas interesadas:

- ha sido **informado** el uso de su información en el momento de la recopilación;
- **puede oponerse** para recibir esta información.

ATENCIÓN

Cada vez que se envía un correo electrónico / SMS / carta, el interesado debe poder oponerse a recibir información relacionada con la vida de la asociación de forma sencilla y gratuita (por ejemplo: insertar un enlace para darse de baja en la parte inferior del boletín o cada correo electrónico enviado).

¿Puede una asociación intercambiar la información de sus miembros con otra asociación con fines de prospección?

Sí, una asociación puede intercambiar la información de sus miembros con otra asociación con fines de prospección.

Tenga en cuenta que las reglas relativas a esta transmisión difieren según el tipo de prospección realizada:

En términos de prospección benéfica, esto solo es posible si los miembros, en el momento de la recolección:

- informado de su uso con fines de prospección;
- informados de su posible transmisión a socios del sector asociativo;
- capaces de oponerse, antes de estos usos, de forma sencilla y gratuita marcando una casilla puesta a su disposición, por ejemplo:

☐ *Me opongo a que mis datos de contacto postales o electrónicos se utilicen para recibir ofertas de la Asociación X por correo postal o correo electrónico.*

☐ *Me opongo a que mis datos de contacto postales o electrónicos se utilicen para recibir ofertas de socios de la asociación X por correo postal o correo electrónico.*

En cuanto a la prospección comercial por medios electrónicos, la normativa aplicable es más exigente: los miembros deben haber prestado explícitamente su consentimiento, al recoger su dirección de correo electrónico, para ser sondeados por la asociación así como para su transmisión a un socio de la Asociación.

PARA IR MÁS LEJOS

Prospección comercial por correo electrónico en cnil.fr

¿Puede una asociación colocar cookies o rastreadores de publicidad en su sitio web?

Sí, cuando se visualiza su sitio web, puede colocar cookies y otros rastreadores en las herramientas utilizadas por los usuarios de Internet (computadora, tableta, teléfono inteligente, etc.) para analizar sus hábitos de navegación y visualización.

Dependiendo del propósito del rastreador que esté utilizando en su sitio, puede ser necesario:

- **informar al usuario de Internet de su existencia** (ex. : cookie de sesión para un teleservicio);
- **para obtener consentimiento** antes de colocar o leer un plotter en su terminal.

Si su sitio utiliza funciones ofrecidas por otros sitios (por ejemplo, soluciones de estadísticas, botones sociales, videos de plataformas de terceros como Google, YouTube, Facebook, etc.), **necesita obtener el consentimiento de los visitantes.**

PARA IR MÁS LEJOS

En cnil.fr:
- Sitio web, cookies y otros rastreadores
- ¿Cómo hago para que mi sitio web cumpla con las normas?

¿Tiene una asociación que realizar una evaluación de impacto de protección de datos (DPIA)?

No, una asociación no debe realizar una DPIA excepto en ciertos casos (por ejemplo, cuando su archivo contiene una gran cantidad de datos confidenciales, o si contiene datos confidenciales relacionados con personas vulnerables, o incluso en el caso de que el archivo impida que las personas vulnerables se beneficien de un servicio).

El análisis de impacto es una herramienta importante para empoderar a las organizaciones: les ayuda no solo a construir un procesamiento de datos que respete la privacidad, sino también a demostrar el cumplimiento de las reglas de protección de datos.

El AIPD se divide en tres partes:

- una descripción detallada del procesamiento implementado, incluidos los aspectos técnicos y operativos;
- la valoración jurídica de las características del tratamiento (objetivos, datos y plazos de conservación, información y derechos de las personas, etc.) y el respeto de los principios y derechos fundamentales que establece la ley;
- el estudio técnico de los riesgos de seguridad de los datos (confidencialidad, integridad y disponibilidad) así como sus potenciales impactos en la privacidad, para determinar las medidas técnicas y organizativas necesarias para proteger los datos.

PARA IR MÁS LEJOS

En cnil.fr:
- Lo que necesita saber sobre la evaluación de impacto de la protección de datos

Comisión Nacional
de Computación y Libertades
3, Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

www.cnil.fr
www.educnum.fr
linc.cnil.fr