GUÍA PRÁCTICA GDPR

DELEGADOS PROTECCION DATOS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil .fr

El objetivo de esta guía es ayudar a ambas organizaciones a establecer la función de delegado de protección de datos y estos delegados en el ejercicio de su profesión.

Esta guía es una herramienta viva que se enriquecerá buenas prácticas comunicadas por profesionales a la Comisión Tecnologías de la información y libertades nacionales.

TABLE DES MATIÈRES

PREFACIO

El trabajo de delegado de protección de datos ("DPD", o "DPO" en esta guía) se ha vuelto esencial desde la entrada en vigor del reglamento europeo de protección de datos (GDPR) el 25 de mayo de 2018. Este reglamento, que armoniza las obligaciones nacionales anteriores a nivel europeo, concierne a las organizaciones en todas sus actividades: gestión de recursos humanos, prospección, relaciones con clientes o usuarios, etc. A partir de ahora, el tratamiento de datos personales es un componente fundamental de la mayoría de sectores de actividad.

Por tanto, es natural que el RGPD dedique tres de sus artículos a definir los contornos de la profesión responsable de asesorar a los responsables del tratamiento de datos sobre la protección de dichos datos. En consecuencia, el DPO adquiere una nueva importancia cualitativa y cuantitativa en comparación con su predecesor en Francia, el Delegado de Protección de Datos (CIL).

El desarrollo es cualitativo, en primer lugar: el espíritu del reglamento es **Hacer del DPO el "director" de la gestión de datos personales en la organización que lo nombra.**. El posicionamiento jerárquico del DPO debe ser testigo de ello, y sus recursos deben adaptarse, para que pueda cumplir plenamente con su trabajo y su rol de piloto de cumplimiento. No debe trabajar en el vacío, sino estar plenamente integrado en las actividades operativas de su organización.**Es un vínculo esencial en la gobernanza de datos.**, en conjunto con el RSSI (responsable de la seguridad de los sistemas de información) y el departamento de TI (departamento de sistemas de información).

El trabajo de DPO también ha cambiado desde un punto de vista cuantitativo. De hecho, el número de OPD ha aumentado considerablemente debido a**la obligación de designación** a los cuales son presentado muchos cuerpos. Así, mientras 18.000 organizaciones tenían un CIL,**más de 80.000 organizaciones habían designado un DPO en 2021**, incluyendo 26.000 en el público.

Plenamente consciente de esta evolución, la CNIL ha adaptado su estrategia de apoyo a las OPD, principalmente orientándola en el desarrollo y apoyo de redes de delegados. Organizados por sectores o regiones, estos responden a un primer nivel de preguntas de campo, interviniendo la CNIL solo en una segunda vez con estos representantes y federaciones.

Complemento la página dedicada al DPO disponible en el sitio web de la CNIL, esta guía tiene como objetivo ayudar tanto a las organizaciones a establecer la función de delegado de protección de datos como a los RPD en el ejercicio de sus misiones.

La guía DPO se divide en 4 capítulos:

- el papel del RPD;
- designación del RPD;
- el ejercicio de las misiones del DPO;
- el apoyo del DPO por parte de la CNIL.

Cada tema está ilustrado por **casos concretos y preguntas frecuentes** relacionados con el tema que se está tratando. El lector también puede confiar en las preguntas frecuentes y en herramientas prácticas, como la carta de compromiso.

Esta guía, cuya redacción se beneficia de tres años de apoyo práctico a las OPD, le proporcionará las claves para aprovechar al máximo la presencia de un delegado, ser contratado como OPD o, de manera más general, mejorar su cumplimiento.

¿CUÁLES SON LAS MISIONES DE LA CNIL?

En Francia, la Comisión Nacional de Informática y Libertades (CNIL) es la autoridad responsable de garantizar la protección de los datos personales. 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 requerir que un actor regularice su tratamiento (notificación formal) o imponga sanciones (multa, etc.).

PARA IR MÁS LEJOS

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

EL PAPEL DEL DPO

El RGPD coloca al DPO como un actor clave en el sistema de gobierno de datos personales. En efecto, las misiones que le son asignadas dedican su rol de piloto del proceso de cumplimiento permanente y dinámico en el que deben registrarse las organizaciones.

FOCUS: LOS TEXTOS QUE DEFINEN LA FUNCIÓN DE DPO

La función del RPD está regulada y definida con precisión en los artículos 37 a 39 del RGPD. Esta guía se basa en este reglamento, la Ley de Protección de Datos y su decreto de ejecución, así como las directrices sobre el DPO del Comité Europeo de Protección de Datos (SEPD). Al final de cada parte, se indica una referencia a los pasajes relevantes de estos textos.

Asesorar y apoyar a la organización

El DPO tiene una función de asesoramiento y apoyo en varios niveles:

- aporta su experiencia a la dirección para que ésta pueda garantizar el cumplimiento del tratamiento;
- Difunde la cultura y las normas de protección de datos a todas las personas que procesan datos personales dentro de la organización.

El RPD puede así identificar y formalizar los momentos clave durante los cuales **quisiera que su intervención o presencia fuera sistemática**, por ejemplo para cada:

- proyecto de decisión para crear o mejorar el procesamiento existente (en particular para garantizar el cumplimiento de los principios de protección de datos desde el diseño y por defecto);
- consideración de la necesidad de una evaluación de impacto de protección de datos (DPIA) y realización efectiva de los mismos;
- redacción o mantenimiento de registro de actividades de procesamiento ;
- redacción y actualización de normas o políticas internas de protección de datos;
- violación de datos personales, con el fin de asesorar sobre las medidas a tomar, así como sobre la notificación a la autoridad ya los interesados.

El DPO crea conciencia y apoya a los actores involucrados en el procesamiento de datos de cada servicio:

- asegurando la adopción por todos de una cultura de "protección de datos personales" (por

ejemplo a través de sesiones de formación internas sobre los principios fundamentales de la protección de datos);

- mediante la realización de acciones de comunicación y sensibilización sobre temas relevantes para la organización (uso de carteles y guías prácticas accesibles desde la intranet, recordatorio de normas de seguridad con motivo de sanción o violación de datos citados en los medios de comunicación, campañas falsas de " *suplantación de identidad* " con fines educativos, etc.);
- presentándose como punto de contacto interno para cualquier cuestión en materia de protección de datos, y en su caso a través de personas de contacto.

Por tanto, el DPO tiene ante todo una misión de información, asesoramiento y control. **No es responsable del cumplimiento de la organización.**, llevar el registro, realizar análisis de impacto o notificaciones de brechas de datos. Sin embargo, está en condiciones de ser un jugador clave cuyas habilidades serán de gran utilidad para el jefe de la organización para ayudarlo a cumplir con sus obligaciones.

ENFOQUE: GESTIÓN DE LA CONFORMIDAD POR PARTE DEL DPO

Asegurar el cumplimiento del RGPD es un proceso activo que consiste en anticipar y organizar las intervenciones del DPO dentro de la organización.
Los pasos a seguir pueden ser, por ejemplo, los siguientes:

- formalizar los casos de consulta del DPO;
- crear, con los departamentos interesados, un "comité GDPR" responsable de arbitrar y orientar las acciones relativas al procesamiento de datos;
- participar en el desarrollo y actualización de documentos de gobernanza (política de seguridad del sistema de información, estatuto de TI, folleto de bienvenida, reglamentos internos, etc.);
- mantener un contacto regular con el personal operativo que procesa datos personales, escucharlos y brindar apoyo;
- prever un procedimiento interno en caso de Control CNIL(procedimientos de recepción, personas a notificar, información a obtener), violación de datos personales (información inmediata al DPO), o bloqueo interno (alerta del responsable del tratamiento y / o resolución del conflicto);
- planificar los métodos de respuesta a solicitudes externas (redactar modelos de respuesta, informar a los servicios en contacto con el público);
- proporcionar una persona de relevo en caso de ausencia o impedimento que pueda recibir solicitudes y ser el punto de contacto interno con las personas interesadas, pero también con la CNIL;
- identificar los servicios relevantes para las actividades regulares y los procedimientos de formación, con la ayuda, si es necesario, de contactos internos o externos competentes;
- mantener un cuadro de mando de las actividades realizadas, con el fin de alimentar un punto regular (reunión de gestión) así como un informe periódico de actividades para la gestión de la organización;
- ser un actor en su red profesional identificando y colaborando con los contactos relevantes del organismo (retransmisores internos, controladores de datos conjuntos, proveedores de servicios);
- mantener sus conocimientos técnicos y operativos en relación con las actividades de procesamiento de la organización a través del seguimiento (sobre la jurisprudencia, publicaciones de las autoridades supervisoras, etc.) y durante la capacitación y el intercambio de experiencias (red geográfica y / o profesional de RPD).

Verifica la efectividad de las reglas.

El DPO es responsable de supervisar el cumplimiento del RGPD.

Esta misión debe revestir la forma de verificaciones organizadas por el DPO (auditoría externa o relevo interno), o llevadas a cabo por el DPO personalmente, en colaboración con otras funciones clave como el CISO (responsable de seguridad de los sistemas de información). Debe ir acompañado de un seguimiento del plan de acción correctivo y evolutivo.

Dependiendo de las prioridades, el propósito de estos controles o auditorías puede consistir en:

- verificaciones de la veracidad de la información contenida en el registro de operaciones de procesamiento implementado por la organización (inventario de actividades de procesamiento, alcance de propósitos, sujetos de datos, tipo de datos procesados, destinatarios y posibles transferencias fuera de la Unión Europea, períodos de retención, medidas de seguridad);
- verificaciones del cumplimiento de las operaciones de procesamiento más sensibles, teniendo en cuenta los análisis de impacto llevados a cabo (en particular con respecto a la implementación de medidas destinadas a reducir la probabilidad y la gravedad de los riesgos);
- la implementación de herramientas para monitorear y controlar el uso del procesamiento (análisis de registros, detección de datos prohibidos, verificación del cumplimiento de los períodos de retención, etc.);
- una verificación de la eficacia de las medidas técnicas y organizativas de protección de datos que la organización se ha comprometido a implementar.

Ser el punto de contacto de la organización en asuntos relacionados con el RGPD.

Con la CNIL

El RPD está, por un lado, obligado a cooperar con la autoridad de control y, por lo tanto, debe desempeñar un papel de "facilitador" durante las discusiones con la CNIL (respuesta a solicitudes durante una inspección in situ, investigación de una queja, consulta dentro del marco de una DPIA, notificación de una violación de datos, etc.).

Además, el DPO puede consultar a la CNIL sobre todas las cuestiones relativas a la protección de datos personales o su función. El responsable del tratamiento o el encargado del tratamiento tiene prohibido enviar estas preguntas para su validación o prohibirlas.

Además, según la Carta de apoyo profesional que publicó en febrero de 2021,**la CNIL no responde a las solicitudes de asesoramiento que le envían organizaciones que no se han preocupado de consultar a su RPD** sobre la pregunta que desean hacer.

La mayoría de las inspecciones in situ de la CNIL se realizan sin previo aviso. Sin embargo, excepcionalmente, la organización y el RPD pueden ser notificados con unos días de anticipación. El DPO puede, durante una verificación in situ, ser "responsable de las instalaciones" donde se encuentran los procesamientos que son objeto de las verificaciones. Es entonces el interlocutor privilegiado, pero no exclusivo, de la delegación de control y se encarga de la revisión y firma del acta redactada al final de la jornada. El responsable del tratamiento sigue estando en condiciones de comentar el informe cuando se le envía.

Por otro lado, el DPO no puede representar al organismo solo ante la CNIL durante una audiencia convocada, porque esto lo colocaría en una situación de conflicto de intereses. No obstante, puede acompañar a un representante de la organización para brindar su experiencia y responder preguntas.

Con las personas afectadas por el tratamiento de datos personales

El DPO también es el punto de contacto para las personas cuyos datos son procesados por el organismo que lo nombró. Como tal, puede encargarse de organizar la tramitación de sus solicitudes para el ejercicio de derechos (acceso, portabilidad, etc.) de forma que se dé una respuesta completa dentro del tiempo asignado. El DPO también podrá ser solicitado por las personas interesadas (empleados, agentes, clientes, proveedores, estudiantes, usuarios, etc.) respecto a cualquier cuestión relacionada con el tratamiento de sus datos personales.

ATENCIÓN

Como parte de una respuesta a una denuncia, el DPO actúa como punto de contacto con la persona interesada y los agentes de la CNIL. **Esto no le autoriza a comunicar los datos de contacto directo de los agentes de la CNIL a terceros.** (incluido el interesado). Estos datos de contacto están destinados al destinatario único de los mensajes enviados y a sus colaboradores.

Asegurar la documentación del procesamiento de datos

La documentación juega un papel preponderante en la nueva lógica de rendición de cuentas (o rendición de cuentas, o incluso " *responsabilidad* ") del RGPD. Obligatorio, permite al responsable del tratamiento o subcontratista garantizar y demostrar el cumplimiento de sus obligaciones así como de las gestiones realizadas.

Se pueden integrar muchos elementos en la documentación, tales como el registro de actividades de procesamiento, DPIA, registro de violaciones de datos y medidas tomadas para remediarlas, avisos informativos, evidencia de la obtención del consentimiento, procedimientos relacionados con el ejercicio de derechos, contratos de subcontratación, herramientas para supervisar transferencias fuera de la Unión Europea. Sindicato, análisis escrito sobre la ausencia de conflicto de interés del RPD, etc. Esta lista no es exhaustiva en la medida en que se puede incluir en la documentación cualquier elemento que permita justificar el cumplimiento y orientar las actuaciones a realizar.

La documentación es una herramienta esencial del DPO porque permite tener un conocimiento exhaustivo de las operaciones de procesamiento implementadas y planificar su gestión. Por tanto, el DPO debe velar por que esta documentación se mantenga, es decir, garantizar su pertinencia y supervisar su actualización.

Con respecto a **mantenimiento de registros de las actividades de procesamiento**, El artículo 30 del RGPD establece que la obligación de llevar un registro pesa sobre el responsable o encargado del tratamiento. Sin embargo, en la práctica, las actividades del DPO pueden llevarlo a hacerse cargo de esta misión. De hecho, el mantenimiento del registro constituye una herramienta de seguimiento y control de las operaciones de tratamiento implementadas, permitiendo al RPD tener el conocimiento más exhaustivo posible de las operaciones de tratamiento y proponer las medidas necesarias para su supervisión. En cualquier caso, debe poder consultarlo en cualquier momento.

Anotar : Se recomienda consignar en la carta compromiso del RPD que llevar el registro es una de sus misiones (si así fuera) e indicar que la información relativa a cada tratamiento le será comunicada por los responsables de los mismos. o quienes las implementan.

Para obtener más información sobre el registro de procesamiento, la CNIL ha publicado una hoja dedicada en su sitio web, que contiene en particular un modelo de registro simplificado, en hoja de cálculo, en formato abierto, de libre reutilización y que se puede adaptar a muchos casos de tratamiento de datos, así como a la Registrarsede la CNIL.

preguntas frecuentes

¿Cómo debe el DPO priorizar sus misiones?

Si bien todas las misiones presentadas anteriormente deben ser implementadas por el RPD, el GDPR especifica que el RPD "tiene debidamente en cuenta, en el desempeño de sus misiones, el riesgo asociado con las operaciones de procesamiento, dada la naturaleza, el alcance, el contexto y los propósitos. del tratamiento "(artículo 39.2). Esto significa que el nivel de vigilancia y recursos debe ser tanto mayor cuanto mayores sean los riesgos que presentan las operaciones de tratamiento (seguimiento riguroso del tratamiento de datos sensibles, formación de empleados especialmente implicados, auditoría interna sobre medidas de seguridad, etc.).

¿El propio RPD tiene que responder a todas las solicitudes externas?

Si la CNIL y cualquier persona interesada deben poder contactar con el RPD en los casos previstos en los textos, no es necesario que este último esté sistemáticamente en el origen de la respuesta. Por otro lado, deberá asegurarse de que cada solicitud reciba el tratamiento adecuado por parte del servicio competente dentro del tiempo asignado.

¿El RPD es responsable del cumplimiento? ¿Son sus recomendaciones vinculantes?

El DPO no es personalmente responsable en caso de incumplimiento de las obligaciones previstas por el RGPD. Es el organismo responsable del cumplimiento del RGPD (ver hoja 6 sobre el estado del DPO). Es imposible transferir al delegado, por delegación de poderes, la responsabilidad que incumbe al responsable del tratamiento o las obligaciones específicas del subcontratista.

Si no se siguen las recomendaciones del DPO, el responsable del tratamiento o el DPO puede documentar de manera útil las decisiones que se han tomado, así como, en su caso, las razones por las que no se siguió la opinión del DPO.

¿Puede el DPD realizar otras misiones distintas a las previstas en el artículo 39 del RGPD?

Es muy posible encomendar al RPD otras tareas siempre que esto no obstaculice el desempeño de las misiones que le asigna específicamente el RGPD (incluso privándolo del tiempo necesario para la ejecución de estas misiones) y no constituyen un conflicto de intereses.

Ciertas tareas parecen estar adaptadas, por naturaleza, a la función del RPD y podrían serle útiles, como llevar el registro de las actividades de procesamiento, participar en la realización o evaluación de evaluaciones de impacto, si las hubiera. Tiene la jurisdicción, o supervisión de casos de violación de datos personales.

Cabe señalar que ninguna de estas misiones puede ser llevada a cabo solo por el RPD, quien necesariamente debe poder trabajar con los equipos procesando o determinando el procesamiento de datos personales. Además, estas obligaciones siguen siendo responsabilidad del responsable del tratamiento o del encargado del tratamiento.

TEXTOS OFICIALES

En cnil.fr:
- Artículos 38 y 39 del RGPD sobre la función y misiones del RPD.
- Artículos 82 y siguientes del decreto de aplicación de la Ley de Protección de Datos, Légifrance.fr.
- La "Carta de Control" de la CNIL.

Hoja 1: ¿En qué casos se debe nombrar un DPD?

Ya sean controladores de datos o subcontratistas, el nombramiento de un delegado es **obligatorio** para :

- autoridades u organismos públicos (con excepción de los tribunales en el ejercicio de sus funciones judiciales);
- organizaciones cuyas actividades básicas les llevan a realizar un seguimiento regular y sistemático de personas a gran escala;
- organizaciones cuyas actividades centrales los llevan a lidiar con informacion delicada o relacionados con condenas y delitos penales.

BUENA PRÁCTICA

Incluso aparte de estos tres casos, **Se recomienda el nombramiento de un DPO tan pronto como la organización encuentre problemas relacionados con la protección de datos personales.**. Esto permite encomendar a un experto la identificación y coordinación de las acciones a realizar en materia de protección de datos.

¿Qué incluye el término "autoridades y organismos públicos"?

Se trata de autoridades nacionales, regionales y locales, pero también organizaciones como estructuras de educación superior, hospitales, agencias de salud, autoridades administrativas independientes (AAI), establecimientos administrativos públicos (EPA), etc.

BUENA PRÁCTICA

Los organismos privados encargados de una misión de servicio público conservan su estatuto de derecho privado y, por lo tanto, no están obligados a designar un RPD. Sin embargo, como se señala en las directrices de CEDP DPO,**Se alienta la designación de un delegado para estos órganos.**incluso en los casos en que no sería obligatorio según los demás criterios.

"Actividad básica": ¿qué es?

La actividad básica de una organización corresponde a su actividad principal. Si el tratamiento de datos personales es fundamental para lograr los objetivos de la organización, entonces se cumple este criterio.

Ejemplo : la actividad básica de una clínica es brindar atención a los pacientes que atiende. Esta actividad implica necesariamente el tratamiento de datos relacionados con la salud (historias clínicas de los pacientes). El tratamiento de estos datos debe, en este caso, ser considerado como una actividad básica de la clínica.

Sin embargo, la actividad de apoyo o "auxiliar" (ejemplo: remuneración de empleados, asistencia informática) no constituye una actividad básica de la clínica.

¿Cómo evaluar el concepto de "gran escala"?

Se trata de un tratamiento cuyo objetivo es tratar "un volumen considerable de datos personales a nivel regional, nacional o supranacional, que pueden afectar a un gran número de interesados y que pueden generar un riesgo elevado" (considerando 91 del RGPD).

No existe un umbral aplicable a todas las situaciones a partir de las cuales se considera que un tratamiento se implementa a "gran escala". Es necesario un análisis caso por caso para evaluar este punto. Este análisis, y el razonamiento detrás de él, pueden incorporarse de manera útil a la literatura.

Debe tener en cuenta un conjunto de factores:

- el número de personas involucradas, en términos absolutos o relativos (en relación con la población en cuestión, y no en relación con la escala de la organización);
- el volumen de datos y / o el espectro de datos procesados;
- la duración o permanencia de las actividades de procesamiento;
- la extensión geográfica de la actividad de procesamiento.

EJEMPLOS

Constituyen tratamientos a gran escala:

- el procesamiento de datos de pacientes por un hospital como parte del curso normal de negocios;
- procesamiento de los datos de viaje de los pasajeros que utilizan el transporte público urbano (rastreado por billetes, por ejemplo);
- el procesamiento de datos de geolocalización en tiempo real de los clientes de una cadena internacional de restaurantes de comida rápida con fines estadísticos por parte de un subcontratista especializado en la prestación de estos servicios;
- el procesamiento de datos de clientes por una compañía de seguros o un banco como parte del curso normal de negocios;
- el procesamiento de datos personales por un motor de búsqueda con fines publicitarios específicos;
- procesamiento de datos (contenido, tráfico, ubicación) por parte de proveedores de servicios telefónicos o de Internet[1].

No constituyen tratamientos a gran escala:

- el procesamiento de los datos de los pacientes por un médico de distrito que trabaje de forma individual si la base de pacientes es de menos de 10,000 personas por año (cf. el sistema de referencia para las prácticas médicas y paramédicas);
- el tratamiento de datos personales relacionados con condenas penales y delitos por un abogado individual.

¿Qué es el “seguimiento regular y sistemático”?

El RGPD no define la noción de "seguimiento regular y sistemático" de las personas, pero da el ejemplo de seguimiento y elaboración de perfiles en línea con fines de publicidad conductual (considerando 24 del RGPD). El SEPD indica que deben tenerse en cuenta uno o más significados para la expresión "regular y sistemático":

- " regular ”debe entenderse como:
  - continuo o que ocurre a intervalos regulares durante un período de tiempo; Dónde
  - recurrente o que se repite en momentos fijos; Dónde
  - teniendo lugar de forma constante o periódica.
- " sistemático ”debe entenderse como:
  - ocurriendo de acuerdo con un sistema; Dónde
  - preestablecido, organizado o metódico; Dónde
  - que se lleva a cabo como parte de un programa general de recopilación de datos; Dónde
  - llevado a cabo como parte de una estrategia.

1 Todos estos ejemplos provienen de Directrices del SEPD sobre el delegado de protección de datos

Ejemplos de seguimiento periódico y sistemático de las personas afectadas:

- actividades de marketing cuya personalización se base en datos personales;
- elaboración de perfiles y puntuación con fines de evaluación de riesgos (evaluación de riesgos crediticios, establecimiento de primas de seguros, prevención de fraudes o detección de blanqueo de capitales, etc.);
- geolocalización por aplicaciones móviles;
- programas de lealtad;
- publicidad comportamental;
- seguimiento de datos de bienestar, salud y estado físico mediante dispositivos portátiles;

- sistemas de televisión de circuito cerrado;
- dispositivos conectados como coches y contadores inteligentes, domótica, etc.

EJEMPLOS DE DESIGNACIÓN DE UN DPO

Partidos políticos : Las actividades principales involucran el procesamiento de categorías especiales de datos (opiniones políticas). Por lo tanto, en vista deartículo 37.1.c del RGPD, el criterio que queda por evaluar para determinar si el nombramiento de un RPD es obligatorio es el carácter "a gran escala" del tratamiento.

Para los partidos políticos activos a nivel nacional y con una gran base de miembros, es probable que se cumpla el criterio de gran escala. Por otro lado, para los partidos pequeños o los partidos locales, este criterio podría no cumplirse. Se debe realizar un análisis caso por caso.

Minorista o gran distribución: la comercialización de productos, el cobro de pagos y posiblemente la gestión de programas de fidelización podrían considerarse actividades fundamentales. Sin embargo, estas actividades pueden no requerir un seguimiento regular y sistemático de las personas afectadas. Por tanto, es necesario realizar un análisis para cada tratamiento para comprobar si este es el caso, en particular en el caso de los programas de fidelización, y así determinar si la designación del RPD es obligatoria.

PARA IR MÁS LEJOS

En cnil.fr:
- Artículo 37,1 del RGPD en casos de nombramientos obligatorios del RPD.
- Considerando 97 del RGPD sobre el concepto de actividad básica.
- Considerando 31 del RGPD sobre la noción de gran escala.
- Considerando 24 del RGPD sobre el concepto de seguimiento del comportamiento de las personas.
- Directrices del SEPD sobre el delegado de protección de datos (pág. 6 y siguientes).

Hoja 2: ¿Quién puede ser designado DPO?

Aunque hay **sin perfil típico** Para realizar la función de DPO, el GDPR requiere que el delegado tenga un cierto nivel de experiencia. La organización también debe asegurarse de que no haya ningún conflicto de intereses con otras misiones.

Conocimientos y habilidades del delegado

La persona contactada para la función de DPO debe tener un cierto **nivel de conocimiento**, es decir :

- experiencia legal y técnica en protección de datos;
- conocimiento del sector empresarial, normativa sectorial y organización de la estructura para la que es designado;
- una comprensión de las operaciones de procesamiento, los sistemas de información y las necesidades de seguridad y protección de datos de la organización;
- para una autoridad pública o un organismo público, un buen conocimiento de las normas y procedimientos administrativos aplicables.

Si la persona contactada no tiene la experiencia en todos estos conocimientos antes de asumir sus funciones, será necesariamente necesario movilizar la experiencia interna y desarrollar sus conocimientos en el muy corto plazo a través de la formación.

La persona también debe presentar las cualidades personales necesarias para esta función: integridad, alto nivel de ética profesional, capacidad para comunicar, popularizar y convencer.

Anotar : el nivel de experiencia requerido varía según la sensibilidad, la complejidad y el volumen de datos procesados por la organización. Estos conocimientos y habilidades se pueden adquirir mediante un plan de formación adaptado al perfil del futuro delegado (ver la pregunta “¿Cómo se puede formar un DPD?”).

ENFOQUE: CERTIFICACIÓN DPO

La certificación es el procedimiento mediante el cual un tercero certifica la conformidad de un producto, un servicio o una habilidad con un estándar o una referencia.

Desde 2018, la CNIL ha aprobado organizaciones que emiten un **Certificación de habilidades de DPO** sobre la base de su índice de referencia, y mantiene una lista de estas organizaciones. Estos ofrecen una prueba, en forma de cuestionario de opción múltiple de al menos cien preguntas relacionadas con la regulación, la responsabilidad y la seguridad.

Esta certificación solo es accesible después de 2 años de experiencia profesional en protección de datos, o 2 años en cualquier campo y formación en el tema de al menos 35 horas. Entonces es válido por 3 años.

Para su titular, la certificación constituye una prueba de su adecuación al requisito de nivel de conocimiento impuesto por el RGPD. Para las organizaciones que buscan perfiles de expertos en "protección de datos", la certificación representa una garantía de confianza.**Sin embargo, no es obligatorio estar certificado para ser designado DPO.**

Sin conflicto de intereses

El DPO puede ejercer otras funciones dentro de la organización (DPO a tiempo parcial). Sin embargo, en el curso de sus otras funciones, no debería haber**poder de decisión sobre la determinación de los fines y medios de procesamiento** : por tanto, el RPD no debería ser "juez y parte".

Se evalúa la existencia de un conflicto de intereses **caso por caso**. Es recomendable documentar el análisis que conduzca a la exclusión de la existencia de un conflicto de intereses para el RPD designado.

Ejemplos de funciones que pueden dar lugar a un conflicto de intereses: director general de servicios, director de operaciones, director médico, director del departamento de marketing, director de recursos humanos, director del departamento de TI, etc.

ATENCIÓN

Las funciones en un nivel jerárquico "inferior" dentro de la estructura organizativa también pueden dar lugar a un conflicto de intereses. **ya que en la práctica la persona participa en la determinación de los fines y medios del procesamiento**.

ENFOQUE: DOCUMENTAR LA ELECCIÓN DE SU DPO

Cuando una organización nombra a un DPO, debe poder demostrar que su **DPO cumple con los requisitos del GDPR** (conocimientos y habilidades, ausencia de conflicto de intereses, etc.).

La CNIL no verifica estos requisitos previos en el momento de la designación. Según el principio de *responsabilidad*, depende del organismo que designe un DPO reunir la documentación interna para certificar que el delegado designado cumple con los requisitos del RGPD. En caso de control por parte de la CNIL, se podrá solicitar a la organización que presente esta documentación.

Ejemplos: CV, descripción del puesto, análisis escrito sobre ausencia de conflicto de intereses, posible certificación, etc.

preguntas frecuentes

¿Qué perfil necesitas tener para ser DPO?

No existe un perfil de DPO típico. De hecho, según el estudio sobre las OPD realizado por AFPA en colaboración con la CNIL[2], alrededor del 28% de las OPD tienen un perfil de TI, y el mismo porcentaje un perfil legal, el 43% restante proviene de administración, finanzas, cumplimiento, auditoría, etc.

¿Tiene un DPO que justificar un diploma en particular?

No es necesario obtener un diploma específico o seguir una formación específica para ser designado DPO. Sin embargo, el delegado debe tener las habilidades y los conocimientos adecuados para desempeñar sus funciones.

Así, si el DPO no cuenta con un diploma especializado en protección de datos, frecuentemente habrá complementado su formación académica con experiencia profesional o formación continuada en seguridad informática, derecho o cualquier otra materia relevante para el ejercicio de sus funciones.

El responsable del tratamiento que contrate a un DPD debe asegurarse de que el candidato seleccionado tenga los conocimientos especializados necesarios y le permitirá mantener y complementar sus conocimientos.

DPO y RSSI: ¿un conflicto de intereses?

Un gerente de seguridad de los sistemas de información puede ser designado DPO si no tiene, como CISO, poder de decisión para determinar los propósitos y medios del procesamiento de datos personales implementados por su estructura.

DPO y representante de los empleados: ¿un conflicto de intereses?

Se puede solicitar a un representante del personal, en el contexto de una votación, que adopte una posición sobre determinados temas o proyectos relacionados con el tratamiento de datos personales, en particular la gestión del personal. En este caso, puede haber riesgo de conflicto de intereses con la función de DPO. Según el mismo razonamiento, un DPO puede aparecer en un comité de ética o conducta profesional si esto no genera un riesgo de conflicto de intereses.

---

2 " Delegado de Protección de Datos (DPO): una profesión en crecimiento, una función estructurada », Estudio realizado por la división de prospectiva empresarial de AFPA, a solicitud del Ministerio de Trabajo, Empleo e Inclusión (DGEFP), en alianza con la CNIL y AFCDP (2020).

¿Puede el representante en la Unión Europea de un responsable o encargado del tratamiento establecido fuera de la Unión ser designado DPO?

El representante de un responsable del tratamiento o de un encargado del tratamiento que no esté establecido en la Unión no puede, en principio, ser designado RPD para este organismo, ya que esto constituiría un conflicto de intereses.

¿Puede una persona jurídica ser subcontratista y DPO para la misma organización?

No existe una prohibición de principio para un proveedor de servicios, que también es un subcontratista. [3], o DPO designado para su cliente. Entonces sería una prestación de servicios separada que no se llevaría a cabo en el marco de las instrucciones del responsable del tratamiento. Este podría ser el caso, por ejemplo, de una organización que ofrece servicios digitales y un DPO subcontratado.

Sin embargo, un **análisis caso por caso** debe llevarse a cabo para evaluar si es probable que la situación comprometa la independencia del RPD en el desempeño de sus funciones. Este análisis forma parte de la documentación del responsable del tratamiento y del encargado del tratamiento.

En algunos casos, es necesario implementar medidas para garantizar esta independencia. Entonces es aconsejable prestar atención:

- el estatus (público o privado) de los actores en cuestión, no estando los actores públicos sujetos a las mismas limitaciones de lucro;
- la posibilidad de proporcionar diferentes puntos de contacto en el proveedor de servicios (uno como subcontratista, otro como proveedor de servicios / RPD).
- la posibilidad de prever dos contratos separados.

Sin embargo, para no encontrarse juez y parte al mismo tiempo y, por tanto, estar libre de conflictos de interés, la persona que ejerce la función de delegado no debe tener ni el cargo de gerente ni la calidad de principal dentro de la estructura.

¿Puede la misma persona ser un DPO para un controlador de datos y su procesador?

El RGPD no prohíbe que se designe un DPO para un controlador de datos y su subcontratista.

Sin embargo, de acuerdo con un razonamiento similar al presentado anteriormente y teniendo en cuenta el requisito de independencia, se recomienda evaluar si la organización y las medidas tomadas permiten garantizar esta independencia. Estos elementos deben estar incluidos en la documentación del responsable del tratamiento y su subcontratista.

En particular, es necesario definir cómo se puede garantizar esta independencia en momentos en que las dos estructuras pueden tener intereses divergentes, por ejemplo, en el contexto del examen del contrato entre el responsable del tratamiento y el encargado del tratamiento.

---

3 Un subcontratista procesa los datos en nombre, siguiendo las instrucciones y bajo la autoridad de un controlador de datos (por ejemplo, alojamiento, mantenimiento, etc.). .

¿Se puede nombrar al mismo delegado para organizaciones competidoras?

Se podrá designar un delegado externo para organizaciones en situación competitiva, siempre que estas diferentes misiones y tareas no den lugar a conflictos de intereses. De hecho, el DPO está sujeto a una obligación de confidencialidad o secreto profesional y, por lo tanto, puede trabajar para empleadores competidores sin poner en peligro la confidencialidad de cada una de las partes.

¿Podemos designar a un abogado como DPO?

Un abogado puede ser designado DPO de una organización sobre la base de un contrato de servicios (DPO externo). Sin embargo, este abogado no puede representar a esta organización ante los tribunales en casos que involucren a sujetos relacionados con datos personales ya que esta representación podría constituir un conflicto de intereses.

¿Puede un político ser DPO?

Un funcionario electo no puede ejercer las funciones de delegado de la comunidad de la que es elegido debido a un conflicto de intereses. De hecho, este último participa en la toma de decisiones sobre el procesamiento de datos implementado por la comunidad.

¿Puede una secretaria del ayuntamiento ser DPO?

En las comunidades pequeñas, a menudo se recurre a los secretarios del ayuntamiento para que asuman la función de DPO. Sin embargo, la realización de misiones asociadas a veces puede tropezar con dificultades: falta de tiempo para dedicar al tema y riesgo de conflictos de intereses.

Así, antes de proceder con la designación, el alcalde debe asegurarse de que el prospecto DPO no participa en las decisiones relativas a los ficheros utilizados por la comunidad (objetivos y condiciones de ejecución, datos tratados, destinatarios, plazos de conservación, medidas de seguridad, etc.) y que tiene tiempo suficiente para cumplir con sus misiones.

¿Puede un becario o aprendiz ser un DPO?

Aunque esta posibilidad no está explícitamente excluida por el RGPD, parece poco compatible con los requisitos vinculados al ejercicio de la función. Además de las dificultades que podría implicar esta designación en materia de legislación laboral (asignación de un aprendiz a un puesto fijo), cabe señalar que:

- el DPO debe tener “conocimientos especializados” mientras el pasante / aprendiz está en el trabajo para aprender;
- el alumno / aprendiz debería poder beneficiarse de los consejos y comentarios sobre su trabajo, lo que contradice el hecho de que el RPD no debería recibir ninguna instrucción sobre el desempeño de estas misiones;
- La misión del DPO es una misión a largo plazo, tanto en el cumplimiento inicial de la organización como en el seguimiento de nuevos proyectos, lo cual es difícil de conciliar con la duración limitada de una pasantía. Como tal, las directrices del SEPD sobre el RPD recomiendan favorecer los contratos más largos para este puesto.

¿Cómo evaluar la independencia del RPD?

La independencia real del DPO, en su función de análisis y asesoramiento, supone que se respeten dos tipos de imparcialidades:

- imparcialidad objetiva: el DPD no es juez y parte, porque no está obligado a controlar lo que él mismo ha decidido, solo o conjuntamente;
- una imparcialidad subjetiva: el RPD está protegido de influencias guiadas por intereses divergentes, que puedan alterar la libertad de sus posiciones.

¿Cuál es el riesgo de una organización que no designa un DPO?

Una organización que no haya designado un RPD cuando este nombramiento sea obligatorio se expondría a una sanción de la CNIL, que podría concretamente revestir la forma de un llamado al orden, un requerimiento de cumplimiento o una multa administrativa de hasta 10 millones de euros. o el 2% de la facturación anual mundial del ejercicio anterior, el que sea mayor.

TEXTOS OFICIALES

En cnil.fr:

- Artículo 37,5 del RGPD sobre los conocimientos y habilidades del delegado.
- Artículo 38,6 del RGPD sobre la ausencia de conflicto de intereses.
- Pautas del SEPD en relación con el delegado de protección de datos (pág. 13 y siguientes; pág. 19 y siguientes).

Hoja 3: ¿DPO interno o externo? ¿Cómo agrupar la función?

Cada organización es libre de organizar la función de DPO de acuerdo con sus necesidades. Esta es una elección que pertenece a la entidad, dependiendo en particular de las ventajas y desventajas de utilizar un RPD externo o interno, la oferta interna disponible y la organización de la estructura.

DPO interno

El delegado puede ser un miembro del personal de la organización. Puede realizar sus funciones a tiempo completo o parcial.

Ventajas :

- conocimiento de la organización de la estructura, los servicios y el sector de actividad;
- proximidad a contactos internos;
- mejor reactividad en caso de solicitud interna sobre temas relacionados con la protección de datos;
- más fácil de predecir su presencia en caso de un control CNIL.

Punto vigilante:

- riesgo de conflicto de intereses si el delegado realiza otras funciones;
- asignación de tiempo suficiente al delegado;
- posicionamiento jerárquico adecuado;
- cualquier plan de formación adaptado al perfil del RPD a planificar.

DPO externo

La función de DPO puede ejercerse sobre la base de un contrato de servicios celebrado con una persona física (ejemplo: consultor, empleado de una filial del grupo, etc.) o jurídica (ejemplo: despacho de abogados, firma consultora, centro de gestión, mixta). unión, etc.).

Ventajas :

- solución a la falta de recursos humanos internos;
- uso de la experiencia y herramientas desarrolladas por el delegado externo;
- especialización del DPO en un sector;
- conocimiento de buenas prácticas para organizaciones similares.

Punto vigilante:

- organización de puntos de intercambio y contactos regulares con el más alto nivel gerencial, así como con los equipos comerciales para mantener la proximidad;
- hacer contacto con el RPD externo de forma tan sistemática, simple y fácil como el contacto con una persona interna;
- dificultad para elegir un proveedor y garantizar su experiencia

DPO compartido

Tanto si se trata de un delegado interno como externo, un DPO puede ser compartido, es decir designado para varias entidades.

Ventajas :

- suavización de los costes vinculados al nombramiento del delegado para las entidades del mismo grupo;
- estandarización de procedimientos entre las entidades que han agrupado la función;
- Gestión transversal del cumplimiento entre organizaciones con las mismas inquietudes.

Punto vigilante:

- organización de puntos de intercambio y contactos regulares con equipos comerciales para mantener la proximidad;
- riesgo para el delegado de no ser informado sobre asuntos internos relacionados con la protección de datos;
- establecimiento de una organización para asegurar un monitoreo eficiente del cumplimiento (por ejemplo: relevos, referentes).

La agrupación es posible bajo **ciertas condiciones** que varían según el tipo de estructura:

- **para el sector privado:** un grupo de empresas puede designar un solo RPD siempre que sea **fácilmente accesible desde cualquier lugar de establecimiento**.

EJEMPLOS

En el caso de un grupo formado por 6 filiales ubicadas en diferentes Estados miembros de la Unión Europea, se podrá designar un único delegado (empleado de una de las filiales o prestador de servicios externo) para la matriz y todas las empresas del grupo. siempre que se establezca una organización adecuada.

Al no estar físicamente presente en cada una de las filiales, el delegado puede, por ejemplo, ser apoyado por una red de “relevos” o “referentes” encargados en particular de brindar apoyo operativo al DPO, al tiempo que le transmiten las preguntas que surjan. .

- **para el sector público:** la función de delegado puede ser compartida entre varias autoridades u organismos públicos, **dada su estructura organizativa y tamaño**.

La puesta en común es una solución especialmente adecuada para **las autoridades locales más pequeñas**. Les permite reducir los costos financieros asociados a la función, mientras se benefician de los servicios de profesionales con habilidades y libertades de TI, conocimiento de los temas específicos del sector público local y la disponibilidad necesaria para un ejercicio efectivo de las misiones.

Puede, en particular, intervenir a nivel de un establecimiento público de cooperación intermunicipal, como una comunidad de municipios o aglomeración, o de un operador público de servicios digitales, como un sindicato mixto, una agencia técnica departamental o un centro de servicios.gestión del servicio público territorial acompañando el desarrollo de la e-administración en su territorio.

Las administraciones locales, los establecimientos públicos locales y los organismos privados responsables de una misión de servicio público que opten por la mutualización deberán celebrar un acuerdo que defina las condiciones en las que se lleva a cabo.

Para obtener más información sobre la puesta en común de iniciativas dentro de las autoridades locales

Ver las hojas " ¿Cómo se ven afectadas las autoridades locales y regionales por el reglamento europeo de protección de datos? " y " Designar un responsable de protección de datos en una comunidadé ”en el sitio web de la CNIL (sección“ Autoridades locales ”).

FOCUS: EL ACUERDO DE MUTUALIZACIÓN PARA ORGANISMOS PÚBLICOS

Las autoridades locales, los establecimientos administrativos públicos locales y las personas jurídicas de derecho privado que gestionen un servicio público que opten por la mancomunación tienen la obligación de celebrar una **acuerdo de mutualización** (Arte. 84 del decreto de desarrollo de la Ley de Protección de Datos).

Este acuerdo define las condiciones bajo las cuales se lleva a cabo esta agrupación.

4 " Delegado de Protección de Datos (DPO): una profesión en crecimiento, una función estructurada », Estudio realizado por la división de prospectiva empresarial de AFPA, a solicitud del Ministerio de Trabajo, Empleo e Inclusión (DGEFP), en alianza con la CNIL y AFCDP (2020).

preguntas frecuentes

DPO interno: ¿a tiempo parcial o completo?

Esta es una decisión que se deja a la discreción del controlador de datos o del procesador que designa un DPO.

La designación de un delegado a tiempo parcial requiere una evaluación de su carga de trabajo con el fin de asignarle el tiempo necesario para el desempeño de sus misiones (ver hoja n ° 5).

Según el estudio realizado por AFPA en alianza con la CNIL[4], solo una cuarta parte de los OPD internos llevan a cabo esta misión a tiempo completo.

¿Se puede nombrar a un DPO por un tiempo limitado?

Las organizaciones para las que la designación de un delegado no sea obligatoria podrán disponer que el RPD, interno o externo, desempeñe sus funciones por un período limitado. Sin embargo, esto debe ser suficiente para que pueda realizar un trabajo en profundidad sobre el cumplimiento que, en la gran mayoría de los casos, requiere varios meses o incluso varios años. La disponibilidad temporal a largo plazo puede ser uno de los recursos que la organización proporciona al DPO. Es recomendable formalizar este punto en la carta compromiso o en el contrato de servicios.

DPO externo: ¿cuáles son los requisitos con respecto a los empleados del organismo de DPO designado?

Cuando la función de delegado la realiza un proveedor de servicios externo, un equipo de personas que trabajan en nombre de esta entidad puede, de hecho, realizar las misiones de delegado como grupo. En este caso, es recomendable prever, en el contrato de servicios, una clara distribución de tareas dentro del equipo externo responsable de la función DPO e identificar claramente a la persona que actúa como contacto a cargo del cliente.
También se recomienda que cada empleado del prestador de servicios que ejerza las funciones de DPO cumpla con todos los requisitos aplicables (independencia, recursos y medios suficientes, ausencia de conflicto de intereses, etc.).

DPO compartido: ¿cómo nombrar a la CNIL?

Si la función de DPO se agrupa para un grupo de entidades, cada una de estas entidades debe, como controlador de datos o subcontratista, completar un formulario de designación de delegado.

Para entidades con un gran número de designaciones a realizar, se propone un procedimiento de designación específico (“designación múltiple”) (para más información, contactar con el servicio de DPO de la CNIL).

TEXTOS DE REFERENCIA

En cnil.fr:
- Artículo 37,6 del RGPD sobre el nombramiento de un delegado interno o externo.
- Artículos 83 y 84 del decreto n ° 2019-536 de 29 de mayo de 2019 sobre los procedimientos para la designación del DPO ante la CNIL y el convenio de mutualización profesional.

Ficha 4: ¿cómo nombrar un DPO?

Paso 1: elija el "DPO correcto"

Un DPO externo puede ser una persona física o jurídica, pero un DPO designado internamente solo puede ser una persona física (un empleado, por ejemplo).
El procedimiento de nombramiento interno de un DPD requiere que primero te preguntes por la persona propuesta para este puesto: en este sentido, es importante que te hagas las preguntas adecuadas para, posteriormente, poder justificar tu elección.

La elección de un RPD interno debe tener en cuenta, en particular:

- el interés de la persona a la que se dirige por las misiones del RPD y el apetito por cuestiones de protección de datos;
- su perfil en cuanto a sus calificaciones y su ausencia de conflictos de interés (ver hoja n ° 2);
- las condiciones para el desempeño de sus misiones (recursos suficientes, acceso a información útil e independencia - ver hojas n ° 5 y 6).

NOMBRAR UN DPO: LAS PREGUNTAS CLAVE

El documento "Las preguntas clave que debe hacerse al nombrar un DPO" (anexo n ° 1) permite verificar que se cumplen los requisitos del RGPD sobre un futuro delegado.

Paso 2: formalizar la designación

Se recomienda formalizar las misiones encomendadas al DPO a través de un documento específico. Ejemplos: carta de compromiso, modificación del contrato de trabajo, descripción del puesto, contrato de servicio para el DPD externo, etc.

Este documento también puede ser una oportunidad para definir los métodos de trabajo del RPD (recursos asignados, intermediarios identificados, frecuencia de reuniones con la dirección de la organización y los servicios que procesan los datos, circuito de comunicación, etc.) describiendo cómo las obligaciones de el organismo designante se traducirá en la práctica.

EJEMPLO DE CARTA DE MISIÓN

Esta guía proporciona un ejemplo de una carta compromiso que se presentará al RPD (ver Anexo 2). Este último debe, por supuesto, adaptarse y concretarse en función de las misiones encomendadas al delegado y de las condiciones de ejercicio de su función.

Paso 3: dé a conocer su DPO

El nombramiento de un DPD debe ir acompañado de **acciones de comunicación** capaz de dar visibilidad a la función y los datos de contacto del delegado dentro de la organización, por ejemplo frente a todos los empleados (agentes o empleados), órganos de representación de los empleados y comités de gestión u órganos ejecutivos.
Ejemplos de acciones de comunicación: nota informativa enviada por la dirección a todo el personal, nota interna publicada en la intranet o por publicación (ver, por ejemplo, el cartel de la CNIL " Adopta los 6 buenos reflejos »), Presentación interna a órganos de dirección, publicación de la carta compromiso, etc.

El propósito de este tipo de acciones es comunicar internamente sobre el rol del RPD, su estado, los recursos que se le asignan y los procedimientos asociados al desempeño de sus misiones. También es una oportunidad para recordar el tema del cumplimiento y presentar los proyectos futuros que serán gestionados por el DPO.

Anotar : el delegado está en contacto permanente con los servicios y departamentos de la organización. Por tanto, este plan de comunicación es especialmente importante en la medida en que proporciona al RPD las condiciones más favorables para asumir su cargo.

Paso 4: designe a su DPO ante la autoridad supervisora competente

Antes de proceder con la designación de su delegado, una organización que trabaje en varios países debe asegurarse de que la CNIL sea la autoridad competente para la designación (ver la pregunta "¿A qué autoridad supervisora designar mi DPO?"). Si es la CNIL, entonces puede proceder a ladesignación en línea de su delegado.

La designación del DPO con la CNIL solo se puede hacer en línea a través del teleservicio dedicado. No se procesa correo postal y no es necesario enviar documentos acreditativos como una deliberación del ayuntamiento que designa al delegado.

Las 4 etapas del formulario de nominación se detallan en el apéndice 3 de esta guía.

preguntas frecuentes

¿Se puede designar parcialmente a un DPO?

El RPD es designado para todas las operaciones de tratamiento realizadas por el responsable o encargado del tratamiento (punto 2.1 de las Directrices del SEPD sobre RPD). Por lo tanto, la designación parcial de un DPO (ejemplo: designación de un DPO solo para procesos de RR.HH.) no es posible.

¿Pueden varias personas desempeñar el papel de RPD?

Una organización solo puede designar a una persona como delegado de protección de datos. Sin embargo, este último puede contar con el apoyo de un equipo, trabajar en colaboración con el resto de líneas de negocio de la organización o disponer de una red de "retransmisores de TI y Libertades" capaces de ayudarlo a concienciar sobre cuestiones de protección de datos o devolverle preguntas. proyectos o solicitudes de ejercicio de derechos.

¿Es necesario informar a los órganos de representación de los trabajadores del nombramiento del RPD?

La información de los órganos de representación de los empleados no es requerida por la normativa. Sin embargo, esta sigue siendo una buena práctica para garantizar la transparencia y la buena visibilidad del nombramiento del delegado dentro de la organización.

Autoridades locales: ¿la designación del RPD requiere el envío a la CNIL de una deliberación o una orden relativa al ejercicio de la función?

No, no se requiere ningún documento acreditativo para la designación del delegado ante la CNIL. Para las autoridades locales, por lo tanto, no es necesario enviarlo, además de monitorear elprocedimiento en línea Previsto a tal efecto, la eventual deliberación que crea el puesto o el decreto que designe al delegado. Solo elprocedimiento en líneaes necesario para designar un DPO.

¿Cuándo entra en vigor la designación del delegado?

La designación del delegado es efectiva al día siguiente de la validación del formulario de designación en línea por parte de la organización.

¿A qué autoridad supervisora en Europa debo nombrar a mi RPD?

La determinación de la autoridad a la que debe designarse el RPD no depende de la ubicación de este último ni del estado de la empresa matriz o subsidiaria de la organización. Por otro lado, la naturaleza de los tratamientos implementados tiene un impacto:

- **Para tratamientos locales** (implementado por los establecimientos de una organización en un solo país y que afecta notablemente solo a las personas de ese país): el DPO debe ser designado para **la autoridad local competente** con respecto al tratamiento local (sede del responsable o encargado del tratamiento, que corresponde a la autoridad del Estado miembro donde se lleva a cabo el tratamiento local).
- **Para procesamiento transfronterizo:** En caso de que el responsable del tratamiento (matriz o filial) también lleve a cabo un tratamiento transfronterizo, el RPD debe ser designado para **la autoridad principal**.

La autoridad principal es la del país donde se encuentra el establecimiento principal (lugar del domicilio social o lugar del establecimiento en el que se tomarán las decisiones relativas a los fines y métodos de tratamiento). Por lo tanto, con frecuencia también es competente para ciertos tratamientos locales.

EJEMPLO

Un DPO se comparte para un grupo de empresas cuya casa matriz está en Italia y la subsidiaria en Francia. Como DPO de la filial francesa, debe ser nombrado miembro de la CNIL con respecto al procesamiento local y el procesamiento transfronterizo cuyo procesamiento la filial francesa es responsable. La filial francesa no requiere ninguna acción ante la autoridad italiana. Asimismo, la empresa matriz en Italia debe designar este DPO a la autoridad supervisora italiana para su procesamiento local y procesamiento transfronterizo del que es responsable de procesar.

Este razonamiento se aplica tanto si se trata del mismo DPO designado para todas las entidades del grupo (mutualizado) como si se trata de un DPO diferente para cada entidad del grupo.

¿Es posible que un empleado se niegue a ser designado DPO?

Aquí se aplican las normas generales del derecho laboral: si esta designación constituye una modificación sustancial del contrato de trabajo, la persona debe estar en condiciones de rechazarlo. Además de esta regla general, se pueden agregar reglas especiales si, por ejemplo, la modificación del contrato de trabajo estaba prevista en el contrato o si el empleado también es un empleado protegido (representante del personal, por ejemplo).

Las razones que llevan a un empleado a rechazar o desear rechazar la función de RPD (falta de recursos para organizar la función, en particular temporal, falta de conocimientos, etc.) pueden ser una **Indicación grave de que no se han cumplido las obligaciones que incumben a la organización en el momento de la designación del delegado.**s.

TEXTOS DE REFERENCIA

En cnil.fr:

- Artículo 37,7 del RGPD sobre el nombramiento del RPD como autoridad de control.
- Artículos 83 y 84 del Decreto No. 2019-536 de 29 de mayo de 2019 sobre los procedimientos para la designación del DPO ante la CNIL y el convenio de mancomunación.
- Directrices del SEPD sobre la designación de una autoridad supervisora principal de un responsable o encargado del tratamiento.

Ficha 5: ¿Qué recursos deberían asignarse al DPD?

El delegado debe contar con los medios necesarios para el desempeño de sus funciones, lo que significa que debe estar **involucrado en todos los asuntos de protección de datos y tener recursos suficientes**.

La participación del RPD en todos los asuntos relacionados con la protección de datos.

Es fundamental que el delegado o, en su caso, su equipo, intervenga lo antes posible en todos los asuntos relacionados con la protección de datos. La información y consulta del RPD tan pronto como se considere un proyecto de procesamiento facilitará el cumplimiento del GDPR y fomentará un enfoque basado en la protección de datos desde la etapa de diseño (conocido como "por diseño").**El DPD debe ser un interlocutor natural dentro de la organización.**, por ejemplo, al estar asociado con grupos de trabajo dedicados a las actividades de procesamiento de datos dentro de la organización.

Por ejemplo, la organización asegura en particular que:

- Se invita al RPD a participar regularmente en las reuniones estratégicas de la organización que definen los proyectos previos que involucran datos personales;
- se recomienda su presencia cuando se toman decisiones con implicaciones en la protección de datos;
- el DPO puede dialogar y trabajar con funciones que desempeñan un papel importante en la protección de datos, como la persona a cargo de la seguridad de los sistemas de información;
- toda la información relevante se transmite al RPD con la suficiente antelación para que pueda emitir una opinión pertinente e informada;
- la opinión del RPD siempre se tiene muy en cuenta. En caso de desacuerdo, se recomienda, como buena práctica, registrar las razones por las que no se siguió el consejo del RPD;

- Se consulta inmediatamente al DPD cuando se produce una filtración de datos u otro incidente (informe en la prensa, quejas, etc.).

Recursos de DPO

El GDPR establece que la organización debe **Proporcionar al RPD los recursos necesarios para llevar a cabo sus tareas.** (tiempo necesario, acceso a recursos económicos, colaboradores si es necesario); en él**facilitar el acceso a los datos y las operaciones de procesamiento** (facilitado el acceso a otros servicios de la organización) y en él **permitiéndoles mantener sus conocimientos especializados**.

Los recursos del DPO deben adaptarse al tamaño, estructura y actividad de la organización. Por lo tanto, cuanto más complejas o sensibles sean las operaciones de procesamiento, mayores serán los recursos asignados al DPO.

Se recomienda especificar el tipo de recursos asignados al RPD en la carta compromiso, como el compromiso de la organización con el RPD para permitirle realizar mejor sus misiones.

EJEMPLOS DE RECURSOS QUE DEBEN SER SUMINISTRADOS AL DPO

- Reconocimiento y promoción **la función del RPD por parte de la alta dirección** (por ejemplo, a nivel de la junta).
- los **tiempo suficiente** para que el RPD pueda desempeñar sus funciones. Este aspecto es particularmente importante cuando el DPD desempeña sus funciones a tiempo parcial. También se recomienda determinar, junto con el DPO, la estimación del tiempo necesario para el ejercicio de su función (la necesidad es más importante al ingresar a la función), que se defina un plan de trabajo y que las tareas del DPO sean priorizado.
- Soporte adecuado desde el punto de vista de **recursos financieros** (disponer de presupuesto propio o disponible para acciones de sensibilización o para la contratación de un equipo de forma temporal o permanente) y **infraestructura** (locales, instalaciones, equipos).
- **Acceso predeterminado a la documentación legal** involucrar a la organización con terceros en asuntos de procesamiento de datos personales (socios y subcontratistas).
- los **comunicación oficial de la designación del RPD a todo el personal** para que se conozca su existencia y función dentro del organismo.
- LOS'**acceso a herramientas de comunicación interna** en el desempeño de sus misiones con el fin de poder concienciar y capacitar en los requisitos del RGPD (recordatorio de buenas prácticas, reacción en caso de correos electrónicos fraudulentos o brechas de datos, etc.).
- LOS'**acceso a otros servicios**, tales como recursos humanos, legal, informática, seguridad, etc., para que el DPO reciba insumos e información esenciales de estos otros departamentos.
- los **formación continua**. El DPO debe poder mantener sus conocimientos actualizados con respecto a los desarrollos regulatorios y técnicos, particularmente en el campo de la protección de datos. Para aumentar constantemente el nivel de experiencia del RPD, se debe alentar al RPD a participar en la formación, así como en otras formas de desarrollo profesional, como la participación en foros de privacidad, talleres, asociaciones profesionales, etc.
- Dependiendo del tamaño y la estructura de la organización, puede ser apropiado formar un**equipo alrededor del DPO** cuyas tareas y responsabilidades de cada miembro deben estar claramente establecidas. Asimismo, cuando la función del DPO la lleve a cabo un prestador de servicios externo, un equipo de personas que trabajen por cuenta de esta entidad podrá llevar a cabo las misiones del DPO, bajo la responsabilidad de una persona de contacto principal designada por el cliente.

preguntas frecuentes

¿Cómo evaluar los recursos que se asignarán al RPD?

La naturaleza y el volumen de los recursos asignados al DPO varían según el tamaño, la estructura y la actividad de la organización. Por lo tanto, cuanto más complejas sean las operaciones de procesamiento o mayor sea la probabilidad de que infrinjan la privacidad de las personas, mayores serán los recursos asignados al RPD. Por ejemplo, el análisis de proyectos complejos por parte del DPO requiere tiempo para brindar asesoramiento relevante. La estimación de la carga de trabajo debe ser proporcional a las prioridades establecidas. Esta evaluación es fundamental para el correcto ejercicio de las misiones del RPD en beneficio de la organización que lo designa.

La asignación de un presupuesto específico puede ser parte de los recursos materiales disponibles para el delegado. Para cuantificar este presupuesto se pueden tener en cuenta diversos elementos: por ejemplo, las necesidades de formación del futuro DPD, las acciones de sensibilización del personal de la organización, la utilización de prestadores de servicios en caso de ser necesario (abogados, auditores, etc.) o la contribución de otros servicios dentro de la organización.

¿Las cartas enviadas al DPO son confidenciales?

Si el DPO desea que su correo sea abierto para fines de clasificación, también tiene derecho a solicitar el establecimiento de un canal de comunicación estrictamente confidencial (correos registrados "confidenciales" que no se abrirán, correos electrónicos encriptados, etc.). Línea telefónica confidencial , etc.) en particular a los efectos de la comunicación con las personas interesadas en una relación de subordinación con la organización.

¿Cómo garantizar el acceso del DPO a los datos de la organización?

El RPD debe, debido a sus misiones, poder acceder a los sistemas de información de la organización, la documentación contractual y la información procesada.. El responsable del tratamiento deberá asegurarse de que los servicios bajo su autoridad faciliten este acceso a petición del delegado. Debido a lo que está en juego en esta área, es aconsejable que el delegado y el gerente acuerden un documento que formalice los casos y las condiciones en las que se llevará a cabo este acceso (ejemplo: Auditoría, verificación esporádica, examen de una solicitud de derechos). , violaciones de datos, etc.).

El DPO está sujeto al secreto profesional o una obligación de confidencialidad, y su acceso a los datos está sujeto a los mismos principios generales que todos los empleados: debe ser proporcionado, justificado y trazable.

Estas modalidades podrían planificarse para adaptar mejor el acceso a las necesidades del DPO (acceso a datos de lectura / escritura, acceso temporal, posibilidades de extracción de una base de datos, etc.). En ciertos casos específicos sensibles (ejemplo: acceso a archivos sobre el puesto de un empleado, a correos electrónicos, a información altamente confidencial) se pueden establecer reglas específicas con el DPO con el fin de garantizar el desempeño de sus misiones (ejemplo: controles operados por un tercero partido).

Este acceso debe incluir archivos que contengan datos personales, así como aquellos que se supone que no los contienen (las infracciones del RGPD en términos de conservación y confidencialidad son observadas periódicamente por la CNIL en archivos que las organizaciones consideran libres de datos personales).

La organización debe asegurarse de que estos límites y adaptaciones no impidan la finalización satisfactoria de las misiones del DPO.

TEXTOS OFICIALES

En cnil.fr:
- Artículo 38,2 GDPR sobre la obligación de proporcionar recursos al RPD.
- Artículo 39,1 del RGPD sobre las misiones del RPD.
- Artículo 25 del RGPD sobre protección de datos por defecto.
- Pautas del SEPD en relación con el delegado de protección de datos (p. 16).

EL EJERCICIO DE LA FUNCIÓN DE DPO

Hoja 6: ¿Cuál es el estado del DPO?

La independencia del DPO en el ejercicio de sus misiones

El RGPD prevé determinadas garantías destinadas a asegurar que el delegado pueda llevar a cabo sus misiones con un grado suficiente de autonomía e independencia frente al organismo que le designe.

Esta independencia significa que el DPO:

- **No debe recibir instrucción en el desempeño de sus funciones.**, por ejemplo, sobre cómo tratar un tema, cómo investigar una denuncia, sobre los resultados a llevar a una auditoría interna o incluso sobre la conveniencia de consultar a la autoridad de control. Asimismo, no se le puede exigir que adopte un determinado punto de vista sobre un asunto relacionado con la ley de protección de datos como una interpretación particular de la ley.
- **No debe ser objeto de sanción o destitución por el cumplimiento de sus misiones.**, por ejemplo si el delegado aconseja al responsable del tratamiento que realice una evaluación de impacto y este no está de acuerdo, o registra un análisis legal o técnico que contradice el adoptado por el responsable del tratamiento. Sin embargo, cabe señalar que las funciones del delegado pueden ser cesadas por motivos relacionados con la legislación laboral habitual (tales como: robo, acoso, otras faltas graves).
- **Reporta directamente a los más altos niveles de liderazgo de la organización.** para que el nivel en el que se toman las decisiones conozca las opiniones y recomendaciones del RPD. Así, la CNIL recomienda que el delegado elabore y presente al más alto nivel de la organización un informe periódico (por ejemplo, anual) de sus actividades. El DPO también debe poder hablar directamente al más alto nivel sobre un tema específico si lo considera necesario.[5]. Tenga en cuenta que este requisito de informar al más alto nivel no prejuzga el "apego" del delegado para el que el RGPD no incluye un requisito.

Falta de responsabilidad del RPD en caso de incumplimiento del RGPD

El GDPR establece que es el controlador quien debe garantizar y poder demostrar que el procesamiento se lleva a cabo de acuerdo con el GDPR. Asimismo, es el subcontratista el responsable de cumplir con sus propias obligaciones en virtud del RGPD. Desde entonces,**el delegado no es responsable en caso de incumplimiento del RGPD dentro del organismo que lo nombró**.

Por tanto, no es posible transferir al RPD, por delegación de poderes, la responsabilidad que incumbe al responsable del tratamiento o las propias obligaciones del subcontratista derivadas del RGPD. De hecho, esto equivaldría a otorgar al DPO poder de decisión sobre el propósito y los medios del procesamiento, lo que constituiría un conflicto de intereses contrario al GDPR.

5 En este sentido, la Comisión Nacional de Protección de Datos de Luxemburgo consideró en su decisión n ° 23FR / 2021 de 29 de junio de 2021 que una línea de reporte directa o la posibilidad de eludir los niveles jerárquicos intermedios podrían ser medidas proporcionadas para garantizar la autonomía del RPD.

Obligación de confidencialidad / secreto profesional

El delegado debe estar sujeto al secreto profesional o al deber de confidencialidad en el desempeño de sus funciones. Por lo tanto, se debe tener cuidado de incluir dicha obligación en el contrato de trabajo o en la carta de misión del delegado interno o en el contrato de servicios del delegado externo.

Anotar : esta obligación de secreto profesional o confidencialidad no impide que el RPD se ponga en contacto con la autoridad supervisora para recabar su opinión. De hecho, el RGPD establece que el RPD puede realizar consultas con la autoridad supervisora sobre cualquier tema.

preguntas frecuentes

¿Se puede sancionar al DPD en el ejercicio de sus misiones?

El DPO no es penalmente responsable del cumplimiento de su organización.. Sin embargo, como cualquier otro empleado o agente, puede ver comprometida su responsabilidad penal si viola intencionalmente las disposiciones penales de la Ley de Protección de Datos o como cómplice si ayuda al responsable del tratamiento o al subtratamiento a violar estas disposiciones penales.

¿Se puede sancionar civilmente al DPD en el ejercicio de sus misiones?

La hipótesis de la implicación de la responsabilidad civil del DPO por el ejercicio de sus misiones no puede afectar al empleado DPO: en aplicación del principio de responsabilidad del empleador por sus empleados, la acción civil iniciada por un interesado por el El tratamiento de datos en cuestión solo puede interponerse contra el responsable del tratamiento. Por otro lado, en lo que respecta al RPD externo, si este último incurriera en una falta profesional que llevara al responsable del tratamiento a sufrir un perjuicio, este último podría reclamar la responsabilidad del RPD externo y obtener una indemnización. Es por eso que algunas compañías de seguros ofrecen seguros de responsabilidad profesional para los OPD.

¿El DPD puede ser destituido o relevado de sus funciones?

El delegado se beneficia de un estatus específico de independencia (ver hoja n ° 6). No puede ser "relevado de sus funciones ni sancionado por el responsable del tratamiento o el subcontratista por el desempeño de sus funciones" (art. 38.3 del RGPD). Esta disposición significa que no se puede reclamar a un DPO por análisis o comentarios basados en la protección de datos que enviaría a las operaciones de procesamiento de su empleador. Por tanto, más allá del riesgo del tribunal laboral, el despido improcedente de un DPO constituiría una infracción del RGPD.

Sin embargo, el DPO no es un empleado protegido en el sentido legal y no tiene un procedimiento de despido específico previsto en el código laboral.

Como cualquier otro empleado o agente, puede ser despedido por motivos distintos al desempeño de sus funciones como delegado, por ejemplo, en caso de robo, acoso moral u otra falta grave similar.

Finalmente, el organismo que designa a un DPD debe asegurarse de que este último tenga las calificaciones y capacidades que le permitan cumplir con sus misiones. Por lo tanto, puede decidir retirar las misiones de DPO a un empleado que no puede cumplir con las misiones que le asigna el GDPR.

Este procedimiento solo es posible si el empleador se ha asegurado de que la dificultad del RPD para llevar a cabo sus misiones no proviene de una insuficiencia de los medios, en particular temporales, que se le otorgan. Debe documentarse y llevarse a cabo de acuerdo con las condiciones establecidas en el contrato o en su estatuto.

En cuanto al RPD externo, su contrato de proveedor de servicios también puede rescindirse de acuerdo con la ley de contrato o de orden público y de acuerdo con las condiciones allí establecidas.

¿Debería el DPO estar adscrito a un departamento en particular?

El RGPD no especifica el nivel de "apego" del delegado que, por lo tanto, puede depender del departamento de sistemas de información (DSI), el departamento de riesgos, cumplimiento, el departamento legal o incluso la secretaría general de la organización. Independientemente de la sucursal a la que dependa, es importante que el DPO pueda informar directamente al más alto nivel de gestión de la organización para que su asesoramiento sea conocido y tenido en cuenta.

¿Puede el RPD recibir instrucciones (como "realizar una auditoría todos los años") o tener objetivos?

El DPO no puede recibir instrucciones sobre la forma operativa de rechazar sus misiones.

Así, por ejemplo, una organización no puede prohibir que el DPO se ponga en contacto con la CNIL para solicitar asesoramiento, obligarla a aprobar un documento, ni distorsionar o rechazar constantemente la comunicación que un DPO le gustaría enviar a los empleados o agentes de la organización. Sobre este tema, la CNIL ya ha intervenido con organizaciones para recordarles sus obligaciones.

Es posible enviarle solicitudes (como la elaboración de un informe anual, la redacción de una auditoría, etc.) siempre que no le impidan disponer de los recursos necesarios, especialmente en cuanto a disponibilidad, para realizar otras misiones que el RPD considere prioritarias. Estas misiones podrían entonces incluirse en la carta de compromiso.

También puede tener objetivos evaluables, acompañados de los medios suficientes para llevarlos a cabo, siempre que estos se establezcan en consonancia con las acciones que él mismo ha identificado como prioritarias, en particular en el contexto de sensibilización de los equipos internos.

La independencia del RPD no debe entenderse, de hecho, como la posibilidad de que el RPD trabaje de manera opaca, sin comunicación con la dirección u otros servicios sobre los elementos que ha identificado como prioritarios o sobre las medidas que se requieren. 'él tiene la intención de establecer. Es en la libertad operativa para definir estas prioridades y estas medidas donde se refleja la independencia: no significa la ausencia de vínculos, sino la ausencia de instrucciones que tendrían el valor de una orden o un requerimiento en la relación. Empleado o jerárquico .

Finalmente, el DPO puede recibir instrucciones sobre elementos que no se encuadran en el desempeño de sus misiones, como la obligación de tener su licencia validada en una herramienta interna.

¿Se pueden "validar" o modificar los documentos producidos por el DPO?

Al indicar que el DPO no recibe ninguna instrucción sobre el desempeño de sus funciones y que debe poder informar directamente al más alto nivel de gestión, el RGPD permite al DPO producir cualquier documento (elemento de formación, informe, experiencia, etc.) sin interferencias, en particular en la sustancia.

Sin embargo, puede decidir por sí mismo enviar trabajos preparatorios a su jerarquía u otros servicios para recibir comentarios o observaciones que puede optar por tener en cuenta o no.

TEXTOS OFICIALES

En cnil.fr:
- Artículo 38,2 y 38,3 del RGPD sobre la función de DPO.
- Artículos 226-26 al 226-24 del código penal.

Ficha 7: ¿Qué hacer en caso de salida, baja o sustitución del DPO?

El delegado juega un papel central en la protección de los datos de la organización y actúa como punto de contacto tanto para las personas como para la autoridad de control con la que debe cooperar. En consecuencia, la salida o sustitución de un DPO, ya sea permanente o temporal, debe ser anticipada y organizada por el responsable del tratamiento lo antes posible.

Transición interna

Comunicarse internamente: De la misma forma que cuando fue nombrado, la salida y sustitución del DPO debe ser transmitida internamente por todos los medios (ejemplo: nota interna publicada en la intranet, información a los órganos de representación de los empleados, etc.).

En caso de sustitución, esta información se utilizará para comunicar el nombre y los datos de contacto del nuevo DPO.

Seguimiento de archivos en curso: Es imprescindible actualizar los procedimientos que permitan asegurar el seguimiento y la recuperación de los expedientes en curso (ejemplo: seguimiento de una solicitud de ejercicio de derechos, realización de una AIPD en curso, etc.).

Transparencia frente a las personas interesadas

En caso de salida o sustitución, la organización debe asegurarse de que los avisos informativos, que deben incluir los datos de contacto del DPO, estén actualizados.

Anotar : para evitar esta actualización sistemática de la información, utilice datos de contacto "neutrales" (ejemplo: dirección de correo electrónico genérica, número de teléfono, dirección postal, etc.).

Procedimientos con la autoridad supervisora

En caso de cambio definitivo

El responsable del tratamiento o el subcontratista deberá, a la mayor brevedad posible, informar a la CNIL de la finalización de su cesión de DPO. Operacionalmente, para tramitar un fin de misión, se solicita copiar al representante legal del correo electrónico que informa a la CNIL del fin de la misión (ver dirección en el correo electrónico de confirmación de la cita).

Si el DPO es reemplazado, el organismo debe, dentro del mismo plazo, designar al nuevo DPO (ver hoja 4).

En caso de ausencia temporal

- **Si el DPO ausente es reemplazado oficialmente por otro DPO durante su ausencia**, entonces se requiere una nueva designación de la CNIL (informando al mismo tiempo del final de la misión del DPO ausente);
- **si el DPO no se reemplaza**, es necesario prever una actualización de los procedimientos internos (ejemplo: enrutamiento de correo y llamadas) para garantizar que se atiendan las solicitudes de las personas interesadas o de la autoridad de control. En los casos en que el nombramiento del delegado sea obligatorio para la organización, esta vacante solo podrá ser excepcional y muy limitada en el tiempo.

Anotar : Cuando la CNIL se pone en contacto con una organización, se pone en contacto con el DPO designado oficialmente para sus servicios, independientemente de las reorganizaciones internas implementadas. Por tanto, es importante gestionar la orientación de las llamadas y cartas a las personas adecuadas durante la duración de una cita permanente.

preguntas frecuentes

¿Puede un DPO solicitar el fin de su misión mientras permanece en la organización?

La CNIL recomienda facilitar al tomar posesión del cargo, en la carta de cesión o en el contrato, los términos y condiciones de terminación de la cesión solicitada por el empleado DPO. Esto permite a ambas partes confirmar que el DPO no será penalizado ni obstaculizado por su misión en el transcurso de su carrera, y que puede beneficiarse de las mismas oportunidades de ascenso o movilidad interna que sus compañeros.

TEXTOS OFICIALES

En cnil.fr:
• Artículo 39.1 del RGPD (misiones DPO).
• Artículo 38.3 del RGPD (independencia del RPD).
• Artículos 83 del decreto de desarrollo de la Ley de Protección de Datos. (procedimientos para la designación del DPO con la CNIL).

¿CÓMO APOYA LA CNIL A LAS OPD?

La CNIL apoya a los OPD proporcionándoles varias herramientas, que pueden clasificarse en las siguientes dos categorías:

Herramientas para la formación

- **El sitio** www.cnil.fr **:** constantemente actualizado, contiene una gran cantidad de información, clasificada en particular por procedimientos, temas, tecnologías o textos oficiales. Las publicaciones periódicas de comunicados de prensa y noticias mantienen actualizado el conocimiento. Un motor de búsqueda y una herramienta de "necesidad de ayuda" también permiten responder a solicitudes específicas.
- **Talleres o seminarios web:** son accesibles a todos los profesionales de la protección de datos previa inscripción a través del sitio web de la CNIL. Se centran en un tema (marketing, recursos humanos, investigación en salud, etc.) que examinan en profundidad, dejando también tiempo para preguntas.
- **Formación online (MOOC)**, relativo a los fundamentos de la protección de datos, " El taller de RGPD », Open to all and free, fue publicado en marzo de 2019. Dado el éxito (más de 100.000 cuentas creadas a finales de 2020), esta herramienta pronto será traducida al inglés y enriquecida con módulos temáticos específicos, comenzando con un módulo para autoridades locales.

Las herramientas para encontrar una respuesta

- **Una línea directa:** Los agentes de servicio de DPO están de guardia los lunes, martes, jueves y viernes de 10 a.m. a 12 p.m. el 01 53 73 22 22 (clave 3), reservado para los delegados designados.

- **Una dirección de correo electrónico dedicada:** la dirección del servicio de DPO (que aparece en el correo electrónico de confirmación de la cita) le permite obtener una respuesta por escrito a las solicitudes de asesoramiento para las cuales el delegado no ha encontrado los elementos deseados en el sitio web de la CNIL, o que no pueden ser 'no han sido ya atendido por una red de profesionales de su sector.

En particular, muchos de ustedes se ponen en contacto con nosotros por correo electrónico o por teléfono: por tanto, es fundamental que consulten nuestro sitio web y realicen su propio análisis antes de contactar con nosotros.
De acuerdo con la carta de apoyo de la CNIL, el servicio de DPO dará prioridad a responder preguntas que no puedan responderse en cnil.fr.

- **Redes profesionales de DPO:** son buenas fuentes de respuestas a preguntas de “campo”. Organizados por sectores y regiones, pueden proporcionar comentarios o consejos valiosos. Como parte de su estrategia de diálogo prioritario con los "jefes de red", estas redes profesionales son interlocutores privilegiados de la CNIL.

Herramientas de cumplimiento

- **Un modelo de registro simplificado:** Los DPO suelen estar en el centro de la implementación de esta herramienta, que es obligatoria y esencial para supervisar el cumplimiento (consulte "El DPO y la documentación"). La CNIL ofrece un modelo de registro reutilizable, en formato abierto, que comprende un formulario tutorial, un formulario de lista de tratamientos, un formulario a completar y un formulario de ejemplo. Ella tambien tiene**publicado** su propio registro, se puede utilizar como un ejemplo concreto para comprender los problemas y una posible forma de utilizar esta herramienta.
- Para la realización deevaluación de impacto de protección de datos, la CNIL ofrece una herramienta PIA lista para usar permitiendo pilotar un AIPD de la A a la Z. También publicó guías para apoyar a los responsables del tratamiento y los RPD en esta obligación, así como listas de tratamiento para las que las EIPD son obligatorias o, por el contrario, no necesarias.
- La CNIL publica numerosos documentos, recordando la ley vigente, resumiendo su doctrina o brindando buenas prácticas. Al visitar su sitio con regularidad, el DPO puede tomar nota de la paquetes de cumplimiento, repositorios, pautas, etc.
- Finalmente, al estar en el centro del cumplimiento de la GDPR, el DPO puede encontrar interés en todas las herramientas publicadas por la CNIL, para dialogar de manera efectiva con sus colegas (por ejemplo con el " Guía para desarrolladores de GDPR ") O para comprender mejor las obligaciones que incumben a su organización (como" Guía práctica de periodos de retención Puede permitirlo).

ENFOQUE: "DPO: ¿POR DÓNDE EMPEZAR? "

Acaba de ser nombrado delegado de protección de datos: ¿cuáles deberían ser sus primeras acciones? ¿Cómo priorizar los diferentes proyectos?

La página " DPO: ¿por dónde empezar?»El sitio web de la CNIL te ofrece un plan de trabajo que te permite proceder metódicamente para ayudar a las organizaciones a cumplir con sus obligaciones, en particular proponiendo un plan de apoyo que permita mapear el tratamiento y priorizar las acciones más urgentes.

Estoy buscando un DPO para mi organización, ¿qué debo hacer?

La elección de un DPO puede hacerse dentro de la fuerza laboral de su organización o llamando a un proveedor de servicios que ofrezca sus servicios de DPO (si corresponde, esta persona también es DPO de otras organizaciones, entonces hablamos de DPO compartido).

El organismo que contrata a la persona debe asegurarse de que la persona tenga un conocimiento especializado de la legislación y la práctica de protección de datos. Por tanto, debe tener en cuenta los cursos de formación, largos o cortos, que sigue la persona a la que se dirige, pero también su experiencia y conocimiento del sector. Existen diplomados en protección de datos, pero no son obligatorios ni la única forma de convertirse en DPO o de formarse en estos temas.

Además, con el fin de apoyar a las organizaciones en la identificación del perfil adecuado, la CNIL ha establecido un procedimiento para Certificación de habilidades de DPO sobre la base de un estándares desarrollados por la CNIL. Las certificaciones son emitidas por organismos certificadores aprobados por la CNIL. La lista de estas organizaciones esdisponible en nuestro sitio web.

Para verificar que un DPO está verdaderamente certificado, un reclutador puede comunicarse con el organismo de certificación que otorgó la certificación. La CNIL no tiene una lista de OPD certificados, pero publicauna lista de organismos de certificación aprobados.

¿Qué trae el nombramiento de un DPO si mi organización ya cuenta con un departamento legal responsable de la protección de datos?

Si una organización encuentra problemas relacionados con la protección de datos personales, la CNIL recomienda el nombramiento de un DPO incluso cuando esto no sea obligatorio.

De hecho, un equipo legal, incluso uno competente, no puede sustituir las ventajas del nombramiento de un DPD:

- es un punto de contacto fácil de encontrar y accesible, tanto interna como externamente;
- combina conocimientos jurídicos y seguridad informática;
- su independencia, definida por un texto legal, asegura su imparcialidad y la libertad de sus recomendaciones;
- puede beneficiarse del apoyo y la asistencia de la CNIL.

¿Dónde debería estar ubicado el DPO?

El RGPD no establece un requisito para la ubicación del DPO. Sin embargo, el delegado debe ser **fácilmente accesible** por las personas interesadas y las autoridades de control competentes. Por lo tanto, se recomienda que el DPO esté ubicado en la Unión Europea, esté o no el controlador o procesador establecido en la Unión Europea.

Si la organización no tiene un establecimiento en la Unión Europea, el delegado podrá establecerse fuera de la Unión Europea, siempre que pueda realizar eficazmente sus actividades.

¿Qué idioma debe hablar el DPO?

El delegado debe poder comunicarse eficazmente con las personas interesadas y cooperar con las autoridades de supervisión competentes. Esto significa que estos intercambios deberán realizarse en el idioma o idiomas utilizados por las personas interesadas y las autoridades supervisoras.

Para cumplir con este requisito, el delegado puede, por ejemplo, ser asistido por un equipo de retransmisores locales que podrán responder en el idioma de las personas interesadas.

Las empresas sondean a los profesionales (empresas, administraciones, asociaciones), a veces de forma agresiva, para vender un servicio de asistencia para el cumplimiento del RGPD.

Como recordatorio, la CNIL nunca cobra por un servicio de cumplimiento de GDPR. Nunca solicita el pago inmediato de una suma de dinero en el marco de un control.

La CNIL y la Dirección General de Competencia, Consumo y Control del Fraude (DGCCRF) han publicado una declaraciónpara ayudar a los profesionales a protegerse contra estas prácticas abusivas.

¿El título de "Delegado de protección de datos - DPO - DPD" está reservado para las personas designadas? con la CNIL?

Sí, este título solo puede ser utilizado por personas que sean DPO en el sentido del RGPD y, en particular, designadas para la CNIL. La persona designada tiene derecho a utilizar elLogotipo "DPO" (marca protegida por la CNIL) en el ejercicio de sus funciones.

Los responsables del tratamiento, salvo en los casos de designación obligatoria, que no deseen designar a un responsable de la protección de datos (RPD) de forma voluntaria, podrán contratar a una persona o consultores externos, responsables de misiones relacionadas con la protección de datos personales.

En este caso, es importante asegurarse de que no haya confusión en cuanto a su título, estatus, funciones y misiones. Por lo tanto, se debe indicar claramente en cualquier comunicación dentro de la empresa, así como con las autoridades de protección de datos, los interesados y el público (en general), que esta persona o consultor no tiene el título de Delegado de Protección de Datos.

¿Por qué la CNIL utiliza la abreviatura "DPO" en lugar de "DPD"?

La CNIL todavía usa el nombre de "oficial de protección de datos", la mención "DPO" interviene sólo de manera incidental para abreviar.

La abreviatura de las palabras " *Delegado de protección de datos* " Sin embargo, la designación de la función de delegado en la versión en inglés del GDPR parece necesaria para la accesibilidad de sus producciones, con el fin de tener en cuenta el uso generalizado de esta abreviatura en las profesiones digitales y entre el público en general.

El uso de la abreviatura "DPO" permite a la CNIL, de acuerdo con una de sus misiones, llegar a una gran audiencia utilizando esta abreviatura para buscar en línea publicaciones relacionadas con la función de delegado de protección de datos.

Sin embargo, no hay ninguna restricción sobre el uso de la abreviatura DPD.

¿Cómo se puede formar un DPO?

Para adquirir las habilidades y los conocimientos necesarios para el ejercicio del puesto de RPD, el delegado puede, en particular, contar con todos los recursos disponibles en el Sitio web de la CNIL.

La CNIL también ofrece jornadas de presentación del RGPD y talleres de información temáticos (seguridad, salud, AIPD, etc.), a veces impartidos en forma de webinars. Para consultar las fechas de estos eventos y registrarse, unagendaestá disponible en el sitio web de la CNIL.

En marzo de 2019, la CNIL lanzó su MOOC, " El taller de RGPD », Gratuito y destinado a todos los públicos, pero lo suficientemente rico como para interesar a las OPD en la formación. Pronto se traducirá al inglés y se enriquecerá con nuevos módulos temáticos.

El DPO también puede enfocarse en cursos largos ofrecidos por universidades o escuelas (ver, entre otros, la lista de capacitaciones de DPO realizadas por AFCDP[6] y la página dedicada en el sitio web de SupDPO[7]).

Según el estudio sobre OPD realizado por AFPA[8], los principales contenidos temáticos sobre los que los RPD desean poder formarse son elementos de seguridad informática (cifrado, autenticación fuerte, trazabilidad, etc.), la realización de los primeros análisis de impacto y el conocimiento de los sistemas de información (base de datos, nube, cookies, API, etc.).

6 Asociación francesa de corresponsales para la protección de datos personales.7
Asociación de OPD de Educación Superior, Investigación e Innovación.
8 " Delegado de Protección de Datos (DPO): una profesión en crecimiento, una función estructurada », Estudio realizado por el departamento de prospectiva empresarial de AFPA, a solicitud del Ministerio de Trabajo, Empleo e Inclusión (DGEFP), en alianza con la CNIL y AFCDP (2020).

Anexo n ° 1: Preguntas clave que debe hacerse al designar un DPD

- ☐ ¿La persona contactada conoce los problemas y tiene interés en la protección de datos y las misiones de un DPO?
- ☐ ¿Ha comprobado que la calidad o las misiones preexistentes de la persona abordada no dan lugar a un conflicto de intereses?
- ☐ ¿Tiene la persona el nivel de conocimientos (experiencia jurídica y técnica en protección de datos, conocimiento de las prácticas de la organización y del sector de actividad, etc.) y las habilidades necesarias (capacidad de comunicación, etc.)?
- ☐ Si es necesario, ¿se ha programado un plan de formación para ello?
- ☐ ¿Ha establecido documentación para justificar la elección de su DPO (ejemplo: CV, posible certificación, etc.)?
- ☐ ¿Hay planes para comunicarse internamente (empleados, IRP, etc.) sobre la designación del DPO?
- ☐ ¿Las asignaciones y condiciones para realizar las asignaciones del delegado están formalizadas en una carta compromiso o contrato de servicio?
- ☐ ¿Existen garantías para asegurar la independencia del DPO (no ser sancionado por el ejercicio de sus misiones DPO, no recibir instrucciones en el contexto del ejercicio de sus misiones DPO)?
- ☐ ¿Existe una organización que permita al RPD informar directamente al nivel más alto de la organización?
- ☐ ¿Se ha realizado una evaluación de la carga de trabajo del RPD y las necesidades materiales (infraestructura, personal adicional, etc.)?
- ☐ ¿Se facilitará el acceso a los datos y las operaciones de tratamiento? ¿Podrá el RPD acceder a información útil?
- ☐ ¿Se han establecido métodos de contacto que permitan a las personas interesadas comunicarse fácilmente con el RPD (dirección de correo electrónico exclusiva, línea telefónica, etc.)?
- ☐ ¿Está definido el alcance de las misiones del DPO? (ejemplo: llevar el registro, redactar cláusulas de subcontratación, etc.)?
- ☐ ¿Ha definido la gobernanza (nivel adecuado de mancomunación, establecimiento de relevos o referentes, formalización de las misiones de estos relevos, etc.)?

Anexo n ° 2: Modelo de carta compromiso entregada por la organización al RPD cuando éste toma posesión de su cargo

ATENCIÓN

Este documento es una carta de compromiso modelo genérica que es probable que una organización envíe a su DPO. Debe adaptarse a las especificidades del contexto (naturaleza jurídica de la organización, tipo de actividad, perfil y posicionamiento del RPD) dentro de los límites del rol y misiones del RPD definidos por el RGPD.

[Nombre de la organización] nombrada en la CNIL, el [fecha], Sra. / Sr. [Nombre, Apellido, cargo si aplica], como Delegado de Protección de Datos (DPO) según se define en los artículos 37 y siguientes del Reglamento (UE) 2016/679 de 27 de abril de 2016 sobre protección de datos (RGPD). La CNIL envió un recibo de esta designación el [fecha].

Como tal, la Sra. / M. [Nombre, apellido del RPD] es el encargado de velar por que se respeten los principios y obligaciones vigentes para todos los tratamientos de datos personales que lleve a cabo [Nombre de la organización] o en su nombre. En el desempeño de su misión, toma en cuenta el riesgo asociado con las operaciones de procesamiento, teniendo en cuenta la naturaleza, alcance, contexto y propósitos del procesamiento.

Como parte de sus funciones como DPO, Mme / M. [nombre, apellido del RPD] informa directamente a [organismo / autoridad organismo de gestión]. Tiene acceso a los datos personales y al tratamiento realizado por [Nombre de la organización] o en su nombre. No recibe instrucciones sobre el desempeño de sus funciones ni puede ser sancionado en su carrera por ellas.

Otras misiones y tareas no pueden atribuirse a la Sra. / M. [Nombre, apellido del DPO] sólo en la medida en que no generen situaciones de conflicto de intereses o le priven de los recursos necesarios para el ejercicio de su misión como DPO.

Sra Sr. [Nombre, apellido del DPD] está sujeto a la obligación de [secreto profesional / confidencialidad]. Sin embargo, esta obligación no debe impedirle buscar asesoramiento, en el desempeño de sus funciones, de cualquier autoridad o persona competente.

Responsable de asegurar el cumplimiento de las operaciones de procesamiento de datos personales con las disposiciones relativas a la protección de datos personales, la misión del RPD es en particular:

- informar y asesorar al responsable del tratamiento o al encargado del tratamiento, así como a los empleados,
- supervisar el cumplimiento de estas normativas y las disposiciones de protección de datos,
- proporcionar asesoramiento, previa solicitud, con respecto a la evaluación de impacto de la protección de datos y verificar su ejecución,

- cooperar con la autoridad de control,
- actuar como punto de contacto en asuntos relacionados con el procesamiento de datos personales.

[En la medida en que esto no impida el cumplimiento de las misiones antes mencionadas, el DPO es responsable de las siguientes misiones adicionales, con la ayuda de los servicios involucrados:

- mantener actualizado el registro de las actividades de procesamiento realizadas por [Nombre de la organización] o en su nombre por un subcontratista;
- participar en la realización de análisis de impacto;
- participar en la realización de notificaciones de violaciones de datos personales;
- proporcionar al responsable del tratamiento un informe mensual / semestral / anual sobre las actividades realizadas cada año].

Para que estas misiones puedan llevarse a cabo, [nombre de la organización] se compromete a garantizar que el RPD disponga de recursos suficientes y adecuados. Como parte del desempeño de sus funciones como DPO, Mme / M. [nombre, apellido del DPO] debe:

- acceder a toda la información sobre los proyectos que tienen un impacto en los métodos de procesamiento de datos personales desde el principio (presencia en reuniones interfuncionales y de negocios, etc.);
- acceder al más alto nivel de gestión del controlador;
- acceder a todos los sistemas de información que dan lugar al tratamiento de datos personales por parte de la organización;
- beneficiarse de una formación periódica que les permita mantener sus conocimientos especializados en el ámbito de la protección de datos;
- [disponer de los medios para cubrir las necesidades materiales y humanas necesarias para el cumplimiento de sus misiones].

Se enviará una copia de esta carta compromiso a [todo el personal y / o los órganos de representación del personal y / o los órganos de toma de decisiones de la estructura].

[La confirmación de aceptación de esta carta de compromiso debe hacerse por correo postal acompañada de una copia firmada de esta carta.]

Firma del representante legal de la organización **Firma del DPO**

Anexo n ° 3: Formulario de designación de DPO

El formulario de nominación consta de 4 pasos:

- Paso 1: información sobre el organismo que designa al RPD;
- Paso 2: información sobre el delegado designado;
- Paso 3: la información pública del delegado;
- Paso 4: resumen y envío a la CNIL

El formulario de designación puede ser cumplimentado por el representante legal del organismo que designe al RPD, o por cualquier otra persona específicamente autorizada por el representante legal.

ATENCIÓN

El nombramiento de un DPO tiene consecuencias legales. El incumplimiento de una de las disposiciones relativas al RPD puede ser sancionado. Por tanto, es imperativo que el representante legal del responsable del tratamiento o del subcontratista que designe al RPD sea informado del proceso de designación de un RPD para su organización.

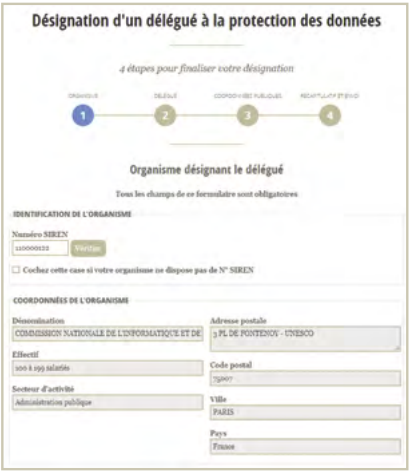
Paso 1: información sobre el organismo que designa al DPD

OPCIÓN 1: LA ORGANIZACIÓN TIENE UN NÚMERO DE SIRENA

La información relativa a su estructura se genera automáticamente a partir del directorio SIRENE del Instituto Nacional de Estadística y Estudios Económicos (INSEE).

Esta información no se puede modificar en el formulario. Pueden existir variaciones en el número de empleados y el sector de actividad, sin que ello repercuta en el nombramiento del delegado.

En caso de información incorrecta (ejemplo: dirección), contacte con los servicios del INSEE o consulte su sitio web www.insee.fr (apartado "registrar una empresa, modificar su situación o declarar su cese").



OPCIÓN 2: LA ORGANIZACIÓN NO TIENE NÚMERO DE SIRENA

Marque la casilla correspondiente.

Debe completar manualmente la información sobre la estructura que designa al delegado.

Anotar : el campo “Contacto CNIL”: si no es el propio representante legal, debe ser una persona en contacto con este último (ejemplo: asistente, subdirector) a quien la CNIL pueda contactar. 'es necesario contactar al representante legal.

Este "contacto CNIL" no puede ser el delegado.

Paso 2: Información sobre el delegado designado

OPCIÓN N ° 1: EL DELEGADO DESIGNADO ES UN INDIVIDUO.

OPCIÓN N ° 2: EL DELEGADO DESIGNADO ES PERSONA JURÍDICA

- O la organización tiene un número SIREN: la información de la organización se genera automáticamente a partir de la base de datos SIRENE del INSEE (ver paso 1).
- O la organización no tiene un número SI-REN: la información debe ingresarse manualmente.

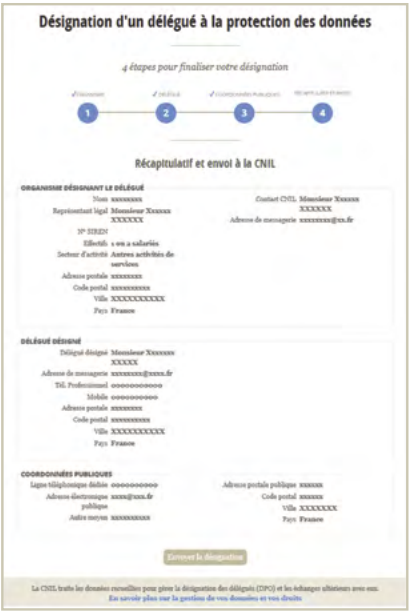
Anotar : " *Datos de contacto de la persona responsable de la designación* ": esta es la persona física interna que realiza las funciones del delegado.

Paso 3: la información pública del delegado

En esta etapa del formulario, se le solicita que complete dos formas de comunicarse con el DPO. Uno de ellos debe ser una dirección de correo electrónico o un formulario en línea.

Estas informaciones se ponen a disposición del público (datos abiertos) desde el sitio web de la CNIL. Por lo tanto, para evitar recibir demasiadas solicitudes, puede ser preferible incluir como punto de contacto electrónico la URL de un formulario en línea.

En cualquier caso, estos datos de contacto públicos no tienen por qué ser idénticos a los datos de contacto solo accesibles a los servicios de la CNIL.



Paso 4: resumen y envío a la CNIL

Antes de validar la designación, recuerde verificar la información proporcionada en el formulario.

Después de la validación, puede descargar un resumen de la designación en formato PDF.

Anotar : el representante legal del organismo que designe al delegado, el contacto del organismo para la CNIL y el delegado designado recibirán un correo electrónico de confirmación.

ATENCIÓN

No es necesario enviar ningún documento adicional a la CNIL (ejemplo: carta compromiso, orden, deliberación, etc.).

En caso de error en el formulario, puede solicitar su corrección enviando un correo electrónico al servicio DPO (cuya dirección aparece en el correo electrónico confirmando la designación del DPO).

APÉNDICE N ° 4: Glosario

DPIA: Evaluación de impacto de protección de datos

API: *Interfaz de programación de aplicaciones* (Interfaz de programación de aplicaciones)

SEPD: Junta europea de protección de datos

DPD / DPO: Delegado de protección de datos / *Delegado de protección de datos*

GDPR: Reglamento general de protección de datos

RSSI: Gerente de seguridad de sistemas de información

Comisión Nacional
TI y libertades
3, place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
Teléfono. : 01 53 73 22 22

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil .fr