ELIOR GROUP

Política de protección de datos de carácter personal

Ámbito	Todos los ámbitos
Versión	V1
Redactor	Comité operativo DCP
Validador	Comité de pilotaje de DCP
Fecha de publicación	01/03/2019
Fecha de actualización	

Introducción

La presente política de protección de datos de carácter personal define la forma en que el Grupo Elior lleva a cabo el tratamiento de datos personales para garantizar la protección de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos de carácter personal.

Dicha política define las normas que todos los colaboradores, colaboradoras, socios, subcontratistas y encargados del tratamiento del Grupo Elior deben respetar a la hora de tratar datos personales.

Cabe recordar que el incumplimiento de las obligaciones relativas a la protección de los datos personales expone al Grupo Elior a una sanción del 4 % de su cifra de negocios mundial lo que, a título indicativo, representa cerca de 268 millones de euros sobre la base de los resultados del ejercicio cerrado el 30 de septiembre de 2018.

En particular, cada una de las personas afectadas deberá velar por:

- el respeto del principio de protección de la privacidad desde el diseño de nuevos proyectos (*privacy by design*) y, en particular, velar por que cada tratamiento de datos (i) corresponda a una finalidad delimitada, (ii) prevea informar a las personas del tratamiento de datos realizado, (iii) defina medidas de protección y (iv) establezca un período de conservación de los datos personales;
- el cumplimiento de los plazos impuestos para responder a las solicitudes de ejercicio de los derechos, a saber, un mes, y la notificación de cualquier fuga de datos a las autoridades competentes en un plazo de 72 horas;
- de manera general, el respeto de los procedimientos y recomendaciones puestos en marcha por la presente política y, en su caso, el contacto con los embajadores de protección de datos de carácter personal o con el equipo GDPR del Grupo Elior, utilizando la dirección gdpr-contact@eliorgroup.com.

Glosario

«**Grupo Elior»** se refiere a la sociedad Elior Group y a todas las sociedades que, en el sentido del artículo L233-3 del Código de Comercio francés,

(i) están bajo el control directo o indirecto de la sociedad Elior Group, o

(ii) están, directa o indirectamente, bajo el control común de la sociedad Elior Group;

«**dato(s) de carácter personal**», «**dato(s) personal(es)** o incluso «**DCP**» se refieren a cualquier información relativa a una persona física identificada o identificable (en adelante denominada la «**persona afectada**»). Se considera como «persona física identificable» a cualquier persona física que pueda ser identificada, directa o indirectamente, en particular en referencia a un identificador como un nombre, número de identificación, datos de localización, un nombre de usuario en línea, o a uno o varios elementos específicos propios de su identidad física, fisiológica, genética, psíquica, económica, cultural o social;

«**tratamiento de datos»** designa cualquier operación o conjunto de operaciones efectuadas o no mediante procedimientos automatizados y aplicadas a datos o conjuntos de datos de carácter personal, como la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, la difusión o cualquier otra forma de puesta a disposición, la conciliación o la interconexión, la limitación, la eliminación o la destrucción de los mismos;

«**responsable del tratamiento»** designa a la persona física o jurídica, la autoridad pública, el servicio u otro organismo que, solo o conjuntamente con otros, determina los fines y los medios del tratamiento; cuando los fines y los medios de dicho tratamiento están determinados por el derecho de la Unión Europea o el derecho de un Estado miembro, el responsable del tratamiento puede ser designado o los criterios específicos aplicables a su designación pueden estar previstos por el derecho de la Unión Europea o por el derecho de un Estado miembro;

«**encargado del tratamiento»** designa a la persona física o jurídica, la autoridad pública, el departamento u otro organismo que trata los datos personales por cuenta del responsable del tratamiento;

«**responsable SI del tratamiento»** se refiere al colaborador del Grupo Elior garante del conocimiento técnico relativo a los recursos informáticos necesarios para el tratamiento, en particular cada tratamiento de datos de carácter personal identificado en el Grupo Elior;

«**responsable sectorial del tratamiento»** se refiere al colaborador del Grupo Elior que define los objetivos y la necesidad del tratamiento para cada ámbito (dirección de proyecto), en particular cada tratamiento de los datos de carácter personal identificado en el Grupo Elior;

«**destinatario»** designa a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo al que se le comuniquen los datos de carácter personal, independientemente de que dicho destinatario sea exterior al grupo Elior o no (terceros). No obstante, las autoridades públicas susceptibles de recibir los datos personales en el marco de una misión de investigación particular no se consideran destinatarios; efectivamente, el tratamiento de datos personales por dichas autoridades se ajusta a las reglas aplicables en materia de protección de datos en función de los fines del tratamiento;

«**consentimiento [de la persona afectada]»** designa toda manifestación de voluntad, libre, específica, informada y unívoca, por la cual la persona cuyos datos de carácter personal son objeto de tratamiento acepta, mediante una declaración o acto positivo claro, que dichos datos sean objeto de un tratamiento;

«**violación de los datos de carácter personal**» se refiere a una violación de la seguridad que trae aparejada, ya sea ilícita o accidentalmente, la destrucción, pérdida, alteración o incluso la divulgación no autorizada de los datos personales transmitidos, conservados o tratados de otra forma, o el acceso no autorizado a dichos datos;

«**normas empresariales vinculantes**» o «**Binding Corporate Rules**» o «**BCR»** designa una política de protección de datos a nivel del Grupo, en el marco de cualquier transferencia de datos personales que se produzca total o parcialmente fuera del Espacio Económico Europeo. Dichas normas son jurídicamente vinculantes y han de ser respetadas por las entidades firmantes de un grupo de sociedades, cualquiera sea su país de implantación, y por

todos los asalariados de una misma entidad jurídica o de un mismo grupo de sociedades. Existen dos tipos de normas empresariales vinculantes: (i) las BCR «responsable del tratamiento», que permiten regular las transferencias efectuadas dentro del grupo que actúa en calidad de responsable del tratamiento, y (ii) las BCL «encargado del tratamiento», que permiten crear un marco de seguridad para las transferencias efectuadas cuando el grupo actúa en calidad de encargado del tratamiento;

«**Evaluación de impacto en la protección de datos**» o **«Data Protection Impact Assessment»** o **DPIA** » significa que el responsable del tratamiento efectúa, antes de cualquier tratamiento que pueda suponer un riesgo elevado para los derechos y libertades de las personas físicas, en particular mediante la utilización de nuevas tecnologías, un análisis del impacto de las operaciones de tratamiento previstas en la protección de datos personales. Un único análisis puede abarcar un conjunto de operaciones de tratamiento similares que presentan riesgos elevados similares.

Índice

1. Contexto

En su calidad de proveedor de servicios de restauración, la seguridad de los alimentos constituye un aspecto fundamental de la actividad del Grupo Elior. Proponer una alimentación sana, elaborada y distribuida de conformidad con la normativa vigente a sus clientes y comensales es una preocupación permanente del Grupo Elior, y constituye uno de los fundamentos de la confianza que de ellos recibe. Del mismo modo, cumplir con la legislación vigente al realizar un tratamiento de datos personales constituye un reto fundamental para el Grupo Elior.

En efecto, la rápida evolución tecnológica y la mundialización han incrementado sustancialmente los flujos de intercambio de datos personales entre los diferentes actores, lo que se traduce en nuevos retos para la protección de los datos personales. El alcance de la recogida y el intercambio de datos personales han aumentado considerablemente, lo que favorece un uso y una valorización de estos datos sin precedentes. El Grupo Elior, que tiene la ambición de diferenciarse gracias a la innovación tecnológica en el ámbito digital y a su capacidad creciente para recoger y explotar datos, se inscribe plenamente en esta tendencia. Los datos, hoy por hoy omnipresentes, son el centro de la cadena de creación de valor. Su buena gestión y seguridad permiten aumentar la eficacia y la competitividad de la empresa, personalizar y consolidar la relación con los clientes y comensales, conquistar nuevos mercados, mejorar los productos y servicios y facilitar la colaboración y la movilidad.

Ahora bien, esto no puede lograrse sin obtener antes la confianza que permita desarrollar el posicionamiento digital del Grupo Elior, garantizando a los equipos, los clientes, los comensales y, más en general, a todos los interlocutores del Grupo Elior que el mismo ejerce un control sobre los datos de carácter personal que les conciernen.

Ante la emergencia de marcos legislativos nacionales y supranacionales, el Grupo Elior vela constantemente por adaptarse a los retos digitales y pone en marcha un proceso de mejora continua y de conformidad de la gestión de los datos personales.

2. Ámbito

En el marco de sus actividades, el Grupo Elior trata constantemente datos personales, por ejemplo:

- al capturar imágenes con cámaras de videovigilancia;
- al tramitar las solicitudes presentadas por los clientes;
- durante la recogida de los regímenes alimentarios de los comensales para servirles comidas apropiadas;
- o al recoger información sobre los equipos en el marco de la gestión de sus carreras.

La presente política se aplica a todos los colaboradores, colaboradoras, socios, subcontratistas y encargados del tratamiento del Grupo Elior cada vez que se recaben, utilicen, hagan accesibles o compartan datos personales de clientes, comensales, equipos, proveedores u otras personas físicas.

Dado que la sede social del Grupo Elior está en Francia, la presente política responde en particular a las obligaciones establecidas por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos, en adelante, el «Reglamento general sobre la protección de datos», el «Reglamento» o el «RGPD».

Esta acción responde a la voluntad de armonizar por lo alto las prácticas del Grupo Elior, de simplificar el seguimiento y mantenimiento de la conformidad a lo largo del tiempo y de garantizar un alto nivel de protección de los datos personales. Para alcanzar este objetivo, la presente política debe tener en cuenta, en la medida de lo posible, las especificidades nacionales:

- en el Espacio Económico Europeo, paralelamente al Reglamento general sobre la protección de datos, cumpliendo con las disposiciones legislativas nacionales específicas que establecen las condiciones en las que el tratamiento de datos personales es lícito;
- fuera del Espacio Económico Europeo, teniendo en cuenta en todos los Estados en los que el Grupo Elior está presente la legislación nacional relativa a la protección de datos personales, y de la autoridad específicamente competente para su aplicación.

Cabe destacar que el derecho a la protección de los datos de carácter personal no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y sopesarse con otros derechos fundamentales, de conformidad con el principio de proporcionalidad, en particular el respeto de la vida privada y familiar, del domicilio y las comunicaciones, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión e información o incluso la libertad de emprendimiento. La presente política no pretende definir el equilibrio entre estos derechos, que deberá ser considerado en cada caso por los servicios jurídicos del Grupo Elior a la vista de la evolución de la jurisprudencia y de las recomendaciones de las autoridades.

3. Gobernanza

A. Marco general

El proceso de control de la gestión de los datos está a cargo de un **equipo del Grupo** compuesto por:

- Un **Group Chief Compliance Officer** (responsable de cumplimiento del Grupo): está directamente subordinado al director general y se encarga de la aplicación de las reglas de cumplimiento. En particular, se ocupa de que la protección de datos personales del Grupo Elior se tenga en cuenta a un nivel óptimo;

- Un **Group Data Protection Officer** (DPO o responsable de la protección de datos): es el responsable de que se aplique el programa de protección de datos personales y de que se cumpla la legislación asociada en todo el Grupo Elior. Conoce en profundidad las actividades y la organización del Grupo Elior, en particular las operaciones de tratamiento, los sistemas de información y las necesidades del Grupo Elior en materia de protección y seguridad de los datos. Ejerce sus funciones y misiones con total independencia y cuenta con el apoyo de un **Group IT Security Compliance Manager** (responsable del cumplimiento de la seguridad TI).

- Un **Group Senior Legal Counsel** (asesor jurídico): acompaña y asesora al DPO, en la comprensión e interpretación de los textos jurídicos y en la relación con las autoridades de protección de datos personales. Asimismo, se encarga de que se tengan en cuenta en las relaciones contractuales los problemas relacionados con la protección de datos personales;

El equipo del Grupo se apoya en actores descentralizados del grupo Elior, a saber: los **embajadores DCP**. Los embajadores DCP son los representantes del DPO dentro de su ámbito y contribuyen en particular:

- a la elaboración de las políticas y procedimientos asociados;
- a garantizar el cumplimiento de la política del Grupo, en particular en lo que se refiere al ejercicio de los derechos y al constante registro de los tratamientos;
- a ser los puntos de contacto preferentes con el equipo RGPD del Grupo y su ámbito para cualquier pregunta relativa a los datos de carácter personal.

La presente política se revisará anualmente, a iniciativa del equipo RGPD del Grupo, para tener en cuenta cualquier evolución de la legislación o de las prácticas internas en el Grupo Elior. Cada una de las filiales del Grupo Elior es libre de organizarse a nivel interno y de adaptar la presente política para facilitar su difusión y aplicación.

B. Herramienta de cumplimiento

El Grupo Elior se ha dotado recientemente de un programa informático de gestión del cumplimiento que permite responder a las obligaciones en materia de protección de datos personales y coordinar los trámites asociados, así como acompañar a sus equipos respetando las reglas de cumplimiento en el marco de sus actividades.

Todos los empleados del Grupo Elior que tengan responsabilidades en materia de tratamiento de datos personales (a saber, los responsables SI y de la actividad, así como los embajadores DCP) tienen acceso a este entorno. Esta herramienta permite en particular:

- mantener actualizados los registros de tratamiento (responsable del tratamiento y encargados del tratamiento);
- acompañar a los responsables de proyecto en la aplicación de los requisitos relativos a la protección de datos;
- generar formularios de contactos para el ejercicio de los derechos de las personas y coordinar su tratamiento;
- mantener un registro de los encargados del tratamiento;
- gestionar las notificaciones de incidentes;
- en general, permitir el cumplimiento de la legislación en el Grupo Elior, de conformidad con el principio de responsabilidad.

No obstante, es responsabilidad:

- de los jefes de proyecto (responsable SI y responsable de la actividad) informar sobre cualquier nuevo tratamiento de datos en este entorno y de los embajadores DCP, acompañar y validar la información facilitada;
- de los embajadores DCP, velar por el correcto tratamiento de las solicitudes de ejercicio de los derechos, con el apoyo de los responsables SI y de la actividad.

C. Comité de pilotaje DCP (CP DCP)

El comité de pilotaje de los datos de carácter personal, coordinado por el DPO bajo la presidencia del Group Chief Compliance Officer, es la instancia de decisión.

El comité posee en particular las siguientes atribuciones en el ámbito de la protección de datos personales en el Grupo Elior:

- validar la política y sus evoluciones;
- elaborar el balance anual de las acciones;
- tomar nota del nivel de cumplimiento;
- validar y decidir la prioridad de las acciones.

De forma complementaria al equipo del Grupo, el CP DCP está compuesto por los miembros siguientes:

- el director de los sistemas de información del Grupo;
- el director jurídico del Grupo;
- el director de auditoría interna del Grupo;
- el director de seguros y prevención de riesgos del Grupo;
- los directores de los sistemas de información de las operaciones;
- los directores jurídicos de las operaciones.

El DPO recopilará formalmente las decisiones del CP DCP al término de los comités. Todas las partes interesadas tendrán acceso a las actas.

El CP DCP se reunirá anualmente. Podrá reunirse de manera extraordinaria con motivo de un evento considerado significativo, a propuesta del DPO (incidente importante, decisión importante, control de las autoridades, etc.).

D. Grupo de trabajo relativo a la protección de datos personales (GT)

El comité operativo DCP, coordinado por el IT Security Compliance Manager y el Group Legal Counsel y presidido por el DPO, es la instancia de planificación y seguimiento de las recomendaciones emitidas por el CP DCP.

Además del equipo del Grupo, también están presentes los embajadores DCP de las zonas (restauración colectiva, restauración concesionaria y servicios) y, si procede, los embajadores DCP a escala internacional.

El CO DCP se reúne cuando la situación así lo exige.

E. Coordinación transversal

El IT Security Compliance Manager se encarga de coordinar la labor relativa a la protección de los datos personales en Francia y a nivel internacional. Asimismo, tiene por cometido identificar y difundir las buenas prácticas asociadas en el Grupo Elior.

4. Nuestras obligaciones

La presente sección describe las diversas obligaciones relacionadas con la protección de los datos personales que incumben al Grupo Elior.

A. Responsabilidad e inventario de los tratamientos

El Reglamento general sobre la protección de datos introduce el principio de responsabilización, o *accountability*, en el marco del tratamiento de datos. Desde su entrada en vigor, el Grupo Elior debe ser capaz de demostrar que cumple con el reglamento, en particular realizando el inventario de los tratamientos de datos aplicados.

Así pues, en el Grupo Elior se deben mantener dos tipos de registros; el primero concierne los tratamientos en los que cualquier entidad del Grupo Elior actúa como responsable del tratamiento; el segundo concierne los tratamientos en los que cualquier entidad del Grupo Elior actúa en calidad de encargada del tratamiento.

Para cada uno de los tratamientos en los que el Grupo Elior actúa como responsable del tratamiento, el registro debe incluir la siguiente información:

- la identidad del responsable del tratamiento y de los encargados del tratamiento;
- la identidad y los datos de los responsables SI y de la actividad;

- la finalidad (el objetivo de la recogida y del tratamiento de datos);
- la base legal del tratamiento;
- la lista de los datos recogidos, el período de conservación y las personas afectadas;
- las categorías de personas que tienen acceso a los datos (administrador, recursos humanos, encargados del tratamiento, etc.);
- la transferencia a un tercer país;
- la forma en que se realiza la información de las personas;
- las medidas de seguridad implantadas;
- eventualmente, los resultados de la DPIA.

Para cada uno de los tratamientos en los que el Grupo Elior actúa como encargado del tratamiento, el registro debe incluir la siguiente información:

- el nombre y los datos de cada cliente en nombre de los cuales se efectúa el tratamiento de los datos;
- el nombre y los datos de cada encargado del tratamiento posterior, en su caso;
- las categorías de los tratamientos efectuados en nombre de cada cliente;
- las transferencias de datos fuera de la UE efectuadas en nombre del cliente;
- en la medida de lo posible, una descripción general de las medidas de seguridad técnicas y organizativas implantadas.

Los responsables SI y de la actividad deben completar este registro con la ayuda de sus embajadores DCP.

B. Transparencia y lealtad

Transparencia

El Grupo Elior y sus equipos tienen el deber de actuar con claridad y transparencia en cuanto al tratamiento de los datos personales. Los datos recogidos no deben utilizarse de una forma y con un objetivo que no sea el razonablemente esperado y previsto en función de la finalidad perseguida.

Por consiguiente, antes de recoger los datos personales, se deben comunicar en lenguaje claro y sencillo los siguientes puntos:

- quiénes somos;
- los datos personales recopilados y su fuente;
- las operaciones que se van a realizar con estos datos personales y su fundamento legal;
- si los datos personales son o van a ser compartidos con otros destinatarios;
- el período de conservación de los datos personales;
- si los datos personales van a ser transferidos fuera del Espacio Económico Europeo;
- los derechos garantizados a las personas en cuanto al tratamiento de los datos personales.

Licitud del tratamiento

Para que un tratamiento de datos personales sea lícito, es necesario contar con razones legítimas, justificar obligaciones legales o haber obtenido el consentimiento de la persona afectada. Así pues, antes de llevar a cabo cualquier tratamiento de datos de carácter personal es necesario, además de informar a las personas, asegurarse de que dicho tratamiento se fundamenta en una de las bases siguientes:

- **Obligación legal**: el tratamiento es necesario para cumplir con una obligación legal a la que está sujeto el responsable del tratamiento (según el derecho nacional o el derecho de la Unión Europea); por ejemplo, la comunicación a la seguridad social y a la administración fiscal de los datos relativos a la remuneración de los asalariados.

- **Necesidad contractual**: el tratamiento es necesario para ejecutar un contrato en el que la persona en cuestión es parte o para aplicar las medidas precontractuales adoptadas a petición de la misma.
  Esta situación debe cubrir únicamente los servicios esenciales para la realización del contrato y, en particular, excluir cualquier acción comercial; por ejemplo, la recogida de los datos de un comensal para la edición y el envío de las facturas o el tratamiento de los datos de los empleados para la elaboración de la nómina.

- **Intereses legítimos**: el tratamiento es necesario para responder a los intereses legítimos del responsable del tratamiento o de un tercero, a menos que prevalezcan los intereses o las libertades y derechos fundamentales de la persona afectada que requieran la protección de los datos personales. Por consiguiente, el interés legítimo del responsable del tratamiento debe sopesarse sistemáticamente con los derechos y libertades fundamentales de las personas afectadas; por ejemplo, la comunicación de elementos relacionados con la corrupción a una autoridad fuera de la Unión Europea o el análisis del

tráfico de Internet para evitar el acceso a sistemas malintencionados, con el fin de garantizar la seguridad de la red informática.

- **Intereses vitales**: el tratamiento es necesario para salvaguardar los intereses vitales de la persona afectada o de otra persona física; por ejemplo, la recopilación de un número de teléfono personal para el envío de un SMS de alerta en caso de acontecimientos graves en el lugar de trabajo o la recogida de datos relativos a un régimen alimentario específico para prevenir cualquier riesgo para la salud de una persona.

- **Interés público**: este fundamento jurídico se refiere a la situación en la que el responsable del tratamiento está investido de una autoridad pública o se le ha encomendado una misión de interés público, para la que es necesario el tratamiento. Si tal situación tuviere lugar, este fundamento jurídico deberá aplicarse en función de cada caso, previa validación por un embajador DCP.

- **Obtención del consentimiento**: la persona afectada debe aceptar el tratamiento de sus datos personales para una o varias finalidades específicas:
    - Su consentimiento debe ser libre (alternativa real, sin consecuencias negativas), específico (un consentimiento específico para cada finalidad), informado (presencia, en el momento de la expresión del consentimiento, de información apropiada y suficiente) y unívoco (lógica de «opt-in», sin ninguna ambigüedad y ausencia de consentimiento por defecto o relacionado con una inacción);
    - la obtención del consentimiento debe poder demostrarse, (por ejemplo: casilla que marcar, formulario que cumplimentar, procedimientos o mecanismos sistemáticos) y se debe dar a la persona la posibilidad de retirarlo.

Minimización de los datos

Además, la información recopilada y registrada debe ser pertinente y estrictamente necesaria para el objetivo perseguido. Así, se deben tomar medidas para reducir al mínimo el volumen de datos de carácter personal recopilados y asegurarse de que son los necesarios para la realización de los fines del tratamiento.

C. Guardar datos exactos y conservarlos durante un tiempo limitado

Conservar información incorrecta o inexacta sobre una persona puede ser perjudicial. Por ejemplo, una persona podría quedar excluida de ciertas ventajas o beneficios relacionados con su estado. Por consiguiente, hay que prestar especial atención al tomar una decisión sobre la base de los datos personales.

Exactitud de los datos

Los colaboradores del Grupo Elior deben asegurarse de que la información de la que se dispone es correcta, lo que es posible garantizar poniendo en práctica los siguientes mecanismos:

- verificar la exactitud de la información en el momento de la recogida, siempre que sea posible;
- en la medida de lo posible, ofrecer a las personas afectadas la posibilidad de actualizar los datos que les conciernan;
- examinar periódicamente los datos personales conservados para asegurarse de que se estén actualizados;
- corregir o suprimir los datos inexactos.

Riesgos inherentes a las zonas de comentarios libres (ZCL)

Los campos de texto y las zonas de comentario deben ser objeto de precauciones particulares. En efecto, los campos de texto libre son útiles para hacer el seguimiento de un expediente o para personalizar una relación. Si bien no está prohibido utilizarlos, su uso debe estar enmarcado por acciones de sensibilización y reglas de gestión para evitar que los comentarios redactados puedan vulnerar los derechos de las personas afectadas.

Efectivamente, algunos comentarios podrían ser despectivos, discriminatorios e incluso ofensivos, o revelar datos llamados sensibles, como la información relativa a la salud. Por tanto, los comentarios deben ser pertinentes, objetivos y respetuosos.

La mejor precaución es tener presente que las personas afectadas (clientes, comensales, empleados, etc.) pueden, en todo momento y previa solicitud, acceder al contenido de estas zonas de comentarios ejerciendo su derecho de acceso.

Período de conservación

Los datos de carácter personal no pueden conservarse de forma indefinida, por lo que debe fijarse un período de conservación en función del objetivo que haya conducido a la recogida de los datos. Una vez alcanzado dicho

objetivo, los datos deben, según el caso, archivarse, suprimirse o anonimizarse (en particular, para elaborar estadísticas).

Cabe señalar que, en aras del interés legítimo del Grupo Elior y de la defensa de sus intereses, dichos datos podrán conservarse durante períodos más largos, si así lo justifica un contexto específico, por ejemplo en el marco de un litigio y, en todo caso, previa notificación al DPO.

D. Garantizar la seguridad de los datos

La seguridad de los datos es un asunto primordial para el Grupo Elior. El hecho de no garantizar la seguridad de los datos a lo largo de todo su ciclo de vida, desde su recogida hasta su destrucción, puede provocar perjuicios importantes para los individuos. Así pues, debe prestarse especial atención a la seguridad de los proveedores externos cuando estos últimos participan en el tratamiento de datos de carácter personal.

Hay numerosas maneras de proteger los datos personales, ya sean electrónicos o en papel. Para acompañar a sus equipos, el Grupo Elior pone a su disposición un corpus documental de última generación, cuya aplicación es obligatoria:

- una política de seguridad de los sistemas de información, acompañada por directivas asociadas que detallan los requisitos que se aplican a los sistemas de información del Grupo Elior;
- las normas de seguridad, que son un requisito previo para cualquier contrato con un proveedor de servicios informáticos.

Las recomendaciones presentadas a continuación se han de adaptar a cada caso particular, en función de los riesgos que el tratamiento de los datos pueda representar para las libertades y la vida privada de las personas afectadas:

- las aplicaciones deben estar protegidas por sistemas de autentificación (nombre de usuario y contraseña), de conformidad con la política de seguridad de la información;
- el acceso a los datos de carácter personal sólo se autoriza a las personas habilitadas para acceder a los mismos, en virtud del derecho a conocer;
- cualquiera sea el tipo de soporte físico, digital o en formato papel, debe estar protegido. Debe prestarse especial atención a los equipos móviles y no dejar sin vigilancia o protección dichos equipos.

En caso de duda, se deberá poner en contacto con el responsable de seguridad de los sistemas de información del Grupo Elior.

E. Subcontratación y transferencia de datos personales

En caso de transferencia de datos de carácter personal, el Grupo Elior debe asegurarse previamente de que la misma sea legalmente posible y segura. La transferencia de datos personales debe interpretarse en sentido amplio; puede tratarse, por ejemplo:

- de transferencias de datos entre entidades jurídicas dentro del propio Grupo Elior;
- de la gestión o mantenimiento externalizados de un recurso informático;
- del alojamiento de un servicio en la nube.

Obligaciones del encargado del tratamiento

De conformidad con el RGPD, el encargado del tratamiento debe acompañar al responsable del tratamiento en su acción constante a favor del cumplimiento. El responsable del tratamiento debe asegurarse de que el encargado del tratamiento cumpla esta misión. El encargado del tratamiento tiene una obligación de:

- **transparencia**: se consigue mediante la redacción de un acto jurídico (i) que defina claramente las obligaciones de cada una de las partes, (ii) que aclare que el encargado del tratamiento sólo actúa previa instrucción del responsable del tratamiento. Esta transparencia también se garantiza llevando un registro actualizado de las actividades realizadas en nombre del responsable del tratamiento y poniendo a disposición toda la información necesaria para demostrar que se cumple con estas obligaciones;
- **asesoramiento y asistencia**: el encargado del tratamiento debe acompañar al responsable del tratamiento a la hora de definir los datos estrictamente necesarios, tratar las solicitudes de ejercicio de los derechos y, más en general, de cumplir con todas sus obligaciones;

- **seguridad**: el encargado del tratamiento debe asegurarse de que sus empleados estén sujetos a una obligación de confidencialidad y debe tomar todas las medidas necesarias para garantizar un nivel de seguridad adaptado a los riesgos y una conservación de los datos durante el plazo estricto previsto;
- **notificación**: el encargado del tratamiento debe notificar al responsable del tratamiento cualquier violación de los datos en un plazo razonable (idealmente 24 o 36 horas).

El Grupo Elior y sus equipos se comprometen a asegurarse del cumplimiento de estos requisitos cada vez que se recurra a encargados del tratamiento y cuando el Grupo Elior actúe como encargado del tratamiento.

Cuando el Grupo Elior actúa como responsable del tratamiento y recurre a uno o varios encargados del tratamiento, estos últimos deben respetar los requisitos del Grupo Elior en materia de protección de datos personales. La transferencia de datos a los encargados del tratamiento debe efectuarse de forma segura. El Grupo Elior tiene la responsabilidad de asegurarse de que sus encargados del tratamiento tomen las medidas adecuadas para garantizar la seguridad de los datos personales.

Las direcciones jurídicas deben ser consultadas sistemáticamente para verificar que cualquier contrato prevea las obligaciones requeridas en materia de protección de datos de carácter personal.

El caso particular de la transferencia fuera del Espacio Económico Europeo (EEE):

La transferencia de datos de carácter personal fuera del EEE debe estar sujeto a mecanismos apropiados, por ejemplo:

- la firma de cláusulas contractuales tipo aprobadas por la Comisión Europea;
- la redacción de reglas de empresa obligatorias: BCR «responsable del tratamiento» o BCR «encargado del tratamiento»;
- la firma de compromisos específicos (por ejemplo: Privacy Shield o escudo protector) para los organismos basados fuera del EEE.

F. Ejercicio de los derechos

El Grupo Elior velará por que las personas afectadas puedan disfrutar plenamente de sus derechos, en particular:

- acceder a los datos personales que les conciernan;
- solicitar la rectificación de los datos personales que les conciernan;
- solicitar la portabilidad de los datos personales que les conciernan en un formato estructurado;
- oponerse a ser objeto de una decisión basada exclusivamente en un tratamiento automatizado;
- solicitar la supresión de los datos personales;
- solicitar la limitación del tratamiento de los datos personales;
- oponerse al tratamiento de los datos personales.

G. Privacy by design

Es más sencillo y menos costoso tomar en cuenta las consideraciones sobre la privacidad y la seguridad de un proyecto lo antes posible. Por ello, desde el inicio de un nuevo proyecto, le corresponde al responsable del proyecto tomar en cuenta la cuestión de la protección de datos de carácter personal, y asegurarse del respeto de la vida privada de las personas afectadas, ya sea al lanzar o un nuevo servicio/producto o al modificarlo.

Ello significa en particular que para cualquier nuevo proyecto, el responsable del proyecto debe:

- identificar los datos de carácter personal susceptibles de estar presentes;
- en su caso:
    - Introducir el proyecto en la herramienta de gestión de la protección de datos personales y seguir las indicaciones,
    - identificar los principales riesgos relacionados con los datos de carácter personal que puedan surgir en el marco de un proyecto particular, sobre todo los riesgos jurídicos, los riesgos relacionados con la reputación y los riesgos para las personas,
    - en el caso del tratamiento de datos de alto riesgo, realizar un análisis de impacto en la protección de datos («DPIA»). Estos tratamientos se refieren en particular a la utilización de datos a gran escala, al uso de nuevas tecnologías, al tratamiento de datos sensibles, a la vigilancia sistemática o a la puesta en marcha de tratamientos con vistas a la toma de decisiones automatizada y la elaboración de perfiles. El Comité Europeo de Protección de Datos indica en su sitio web, país por país, la lista de tratamientos para los que es obligatorio realizar una DPIA,

- asegurarse del cumplimiento de la política del Grupo,
- velar por la aplicación y el control de los mecanismos de protección organizativos y técnicos.

En caso de que se necesite acompañamiento o precisiones, el responsable del proyecto puede dirigirse a sus embajadores DCP.

H. Comunicación y sensibilización

En función de los retos identificados y de las constataciones relativas a la conformidad del Grupo Elior, el equipo del Grupo pone en marcha anualmente un plan de comunicación y de sensibilización, con el apoyo de los embajadores DCP. Este proceso ha de tener por objetivo la instauración de una cultura de la protección de datos personales en el Grupo Elior.

Se invita a los equipos a contribuir a la mejora de la política y de los procesos asociados.

I. Categorías particulares de tratamiento y datos personales

Datos de carácter personal sensibles o asimilados

Se trata de información que revela los orígenes raciales o étnicos, las opiniones políticas, filosóficas o religiosas, la afiliación sindical, la salud o la vida sexual de una persona física. La información relativa a las infracciones o condenas también entra dentro de esta categoría.

En el Grupo Elior se recomienda no recabar ni utilizar estos datos dado su alto riesgo para la vida privada de las personas, salvo en determinados casos concretos:

- si la persona afectada ha dado su consentimiento expreso (claro y explícito, por escrito);
- si estos datos son necesarios con fines médicos o para la investigación en el ámbito de la salud;
- si su utilización está autorizada por la autoridad de protección de datos personales.

Como estos casos pueden variar en función del derecho nacional de cada país, para este tipo de cuestiones conviene ponerse en contacto con los embajadores DCP o con el equipo de RGPD del Grupo. Además, deberá realizarse sistemáticamente una DPIA.

Datos de carácter personal y derecho a la imagen de los niños

Los niños merecen una protección específica en lo que se refiere a sus datos personales, ya que pueden ser menos conscientes de los riesgos, las consecuencias o las garantías que deben aportarse y de sus derechos en materia de tratamiento de los datos personales.

En el marco de los servicios de la sociedad de la información, el tratamiento de los datos personales de un niño es lícito cuando el menor tiene al menos 16 años. Cuando el niño tiene menos de 16 años, este tratamiento sólo es lícito si, y en la medida en que el titular de la responsabilidad parental del niño conceda o autorice el consentimiento. Los Estados miembros pueden prever por ley una edad inferior para estos fines, siempre que no sea inferior a 13 años. No dudar en ponerse en contacto con el embajador DCP para conocer el umbral de edad en función del tratamiento previsto.

Se debe realizar sistemáticamente una DPIA antes de poner en práctica estos tratamientos.

Operaciones de marketing

Las operaciones de marketing deben respetar las decisiones y los derechos de las personas afectadas. Durante las operaciones de marketing, en particular por vía electrónica, cabe asegurarse de que:

- las personas afectadas han dado su consentimiento expreso (para las relaciones BtoC);
- las personas no han ejercido su derecho de oposición a la prospección;
- los mensajes ofrecen la posibilidad de darse de baja fácilmente («opt-out»);
- ningún destinatario puede ver los nombres y los datos de otro destinatario.

J. Violación de datos

A pesar de la aplicación de normas de alto nivel para garantizar la seguridad de los datos, el Grupo Elior no puede protegerse completamente contra el riesgo de violación de datos, que puede definirse como:

- Una vulneración de la confidencialidad, es decir, una fuga de datos (por ejemplo: pérdida del dispositivo USB con archivos de clientes);

- un atentado contra la integridad, es decir una modificación no prevista (por ejemplo: modificación no deseada de la base de datos que indica automáticamente a las autoridades el adjudicatario de un vehículo de función);
- una vulneración de la disponibilidad, es decir, la destrucción de datos (por ejemplo: software malicioso que encripta una base de datos).

La fuente de estas violaciones puede ser tanto interna como externa (por ejemplo: ataque de un recurso del Grupo Elior o de un proveedor expuesto a Internet). También puede ser intencional o accidental (por ejemplo, pantalla no protegida por un filtro de confidencialidad, expuesto en un transporte público).

Es responsabilidad de todos vigilar y notificar inmediatamente cualquier violación de datos al equipo RGPD del Grupo. En caso de que se atente contra la seguridad, de forma comprobada o supuesta, se deberá actuar inmediatamente para limitar los efectos y los daños. En los casos más graves, el Grupo Elior deberá informar a la autoridad de protección de datos competente y facilitarle un plan de acción que permita mitigar el impacto de la violación en un plazo de 72 horas y, en algunos casos, informar también a las personas afectadas.

K. Control y relación con las autoridades de protección de datos

Impacto potencial del incumplimiento de la protección de datos personales

Las infracciones de la legislación sobre la protección de datos personales pueden tener graves consecuencias, en particular:

- sanciones financieras de hasta el 4 % de la cifra de negocios total del Grupo Elior;
- solicitudes de indemnización de las personas afectadas por la violación de la vida privada;
- el cumplimiento bajo multa coercitiva, la limitación de un tratamiento o la suspensión de los flujos de datos;
- el menoscabo de la reputación y la imagen del Grupo Elior.

Poder de las autoridades de protección de datos

El Grupo Elior está redactando las normas empresariales vinculantes o *Binding Corporate Rules*. Dichas BCR tienen por cometido demostrar el respeto de un nivel de protección de datos similar, con independencia del lugar en el que se sitúe la entidad jurídica filial del grupo Elior y autorizar las transferencias de datos personales dentro del Grupo Elior.

La autoridad de protección de datos personales dispone del poder de controlar el cumplimiento del Reglamento general sobre la protección de datos mediante controles físicos o a distancia y puede, en particular:

- obtener una copia del máximo de información, técnica y jurídica, para evaluar las condiciones en las que tiene lugar el tratamiento de los datos personales;
- solicitar la comunicación de todos los documentos necesarios para el cumplimiento de su misión;
- acceder a los programas informáticos y a los datos, y solicitar su transcripción;
- solicitar una copia de los contratos (por ejemplo: contratos de alquiler de archivos, contratos de subcontratación informática), formularios, expedientes en papel, bases de datos, etc.
- realizar a distancia escáneres de vulnerabilidad y auditorías de seguridad, y verificar la presencia de los avisos de información legal.

En Francia, el artículo 51 de la ley nº78-17 de 6 de enero de 1978 modificada relativa a la informática, a los archivos y a las libertades denominada «ley de Informática y Libertades» dispone que cualquier obstáculo a la acción de la Cnil se castigue con un año de prisión y 15.000 € de multa. Se obstaculiza la acción de la autoridad de protección de datos personales en caso de:

- oposición al ejercicio de las misiones confiadas a los miembros o agentes habilitados cuando la visita ha sido autorizada por el juez de libertades y de detención;
- negativa de comunicación, ocultación o destrucción de la información y los documentos útiles para la misión de control;
- comunicación de información no conforme con el contenido de los registros tal y como figuraba en el momento en que se formuló la solicitud de la autoridad de protección de datos personales o presentación de un contenido en una forma a la que no se pueda acceder directamente.

Conducta exigida:

Se recomienda ponerse en contacto inmediatamente con el equipo del Grupo y cooperar plenamente con las autoridades, previa verificación de la identidad de las personas en cuestión (mandato y tarjeta de identidad profesional).

El equipo del Grupo es la única entidad habilitada para comunicarse con las autoridades de protección de datos (por ejemplo: procedimiento previo, solicitud de información, respuesta a las consultas, etc.). Por lo tanto, cualquier solicitud de las autoridades debe serle notificada sin demora.

5. Información complementaria

Si tiene alguna pregunta sobre la presente política o si desea obtener más información sobre cualquiera de los temas tratados, puede ponerse en contacto con el equipo del Grupo mediante la siguiente dirección de correo electrónico: gdpr-contact@eliorgroup.com.