2022

Políticas de Protección de Datos Personales

NAE COMUNICACIONS, S.L.

V_1.3

Contenido

I. Protección de datos personales

a. El Reglamento

A partir del 25 de mayo de 2018, con la entrada en vigor del Reglamento (UE) 2016/679, General de Protección de Datos del Parlamento Europeo y del Consejo, ("RGPD" o "Reglamento"), hay un único conjunto de normas de protección de datos para todas las empresas que operan en la Unión Europea (UE), con independencia de dónde tengan su sede.

El RGPD regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea (UE).

No se aplica al tratamiento de datos personales de personas fallecidas, el que se realice en el ámbito doméstico o personal o a personas jurídicas. Sin embargo, en este último caso, hay que tomar en consideración que aquellos datos relativos a personas de contacto de personas jurídicas si se consideran por la normativa actual como datos de carácter personal.

Las normas no se aplican a los datos que trate una persona por motivos exclusivamente personales o en el marco de una actividad doméstica, siempre que no guarden relación con ninguna actividad profesional o comercial. Cuando una persona utilice los datos personales fuera de la "esfera personal", por ejemplo, para actividades socioculturales o financieras, dicha persona deberá respetar el Reglamento en materia de protección de datos.

b. Datos Personales

Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

Los datos personales que hayan sido anonimizados, de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

El RGPD protege los datos personales independientemente de la tecnología utilizada para su tratamiento; es "tecnológicamente neutro" y se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético). Asimismo, no importa cómo se conservan los datos: ya sea en un sistema informático, a través de videovigilancia o sobre papel, en todos estos casos, los datos personales están sujetos a los requisitos de protección establecidos en el RGPD.

c. Tratamiento

El "tratamiento" abarca una amplia gama de operaciones realizadas sobre los datos personales, que incluyen procedimientos manuales o automatizados. Estas son la obtención, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o

cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales.

El RGPD se aplica al tratamiento de datos personales total o parcialmente automatizado, así como al tratamiento no automatizado, si este forma parte de un fichero estructurado.

d. Política de Protección de Datos

La Política de Protección de Datos de Nae (en adelante, la Política o Políticas), esta formada por lo indicado en este documento, y otra documentación de apoyo que la desarrolla, como procedimientos, guías y protocolos de actuación, de acuerdo con lo previsto en el RGPD y la legislación aplicable en protección de datos española, la cual deberá de ser conocida, aceptada y cumplida por todas aquellas personas afectadas, principalmente, su plantilla y colaboradores autónomos.

II. Principios rectores en la gestión de datos personales

En Nae Comunicacions, S.L. (en adelante, Nae) el tipo y la cantidad de datos personales que se pueden tratar dependerán de las razones legales del tratamiento (base jurídica utilizada) y lo que se quiera hacer con aquellos. En cualquiera de los ámbitos de la actividad que realizamos, aplicamos el máximo rigor en la gestión de los datos personales que tratamos, sobre la base varios principios básicos, entre los cuales se incluyen los siguientes:

- los datos personales deben tratarse de forma lícita y transparente, garantizando la lealtad hacia las personas cuyos datos personales se están tratando ("*licitud, lealtad y transparencia*"),
- deben tenerse fines específicos para el tratamiento de los datos e informarse a las personas de dichos fines al recoger sus datos personales; no pueden recogerse datos personales para fines indeterminados y no se pueden seguir utilizando los datos personales para otros fines que no sean compatibles con la finalidad original de la recogida ("*limitación de la finalidad*"),
- solo deben recogerse y tratarse los datos personales que sean necesarios para cumplir esa finalidad ("*minimización de datos*"),
- debe garantizarse que los datos personales sean exactos y estén actualizados, en relación con los fines para los que son tratados, y corregirlos en caso contrario ("*exactitud*"),
- debe garantizarse que los datos personales no se conserven más tiempo del necesario para los fines para los que fueron recogidos ("*limitación del plazo de conservación*"),
- deben establecerse garantías técnicas y organizativas apropiadas que garanticen la seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de la tecnología apropiada ("*integridad y confidencialidad*").

III. Política de Protección de Datos de la organización

a. Ámbito de aplicación

1. Esta Política regula la forma en que Nae y/o sus entidades (en adelante, referidas todas como la Empresa) recogen, obtienen, utilizan, retienen,

transfieren y procesan los datos personales de los individuos (en adelante, el/los interesado/s). A su vez, también se pretende garantizar que todos los partícipes entiendan las normas sobre la protección de datos personales y los derechos del interesado en relación con sus datos personales tratados por Nae. Asimismo, la Política regula las circunstancias en las que una entidad procesa datos personales en nombre de otra entidad. El contenido de esta Política no anula las normativas o regulaciones europeas o nacionales aplicables en materia de protección de datos en los países en los que opera Nae. Esta Política y su documentación de apoyo no se aplica al tratamiento de datos personales en nombre de los clientes de Nae y de otros terceros durante la prestación de servicios que de dicha relación se deriven.

Algunas entidades de Nae también podrían estar sujetas a variaciones específicas de esta Política. Estas variaciones tienen por objeto regular el tratamiento de datos personales de conformidad con las leyes locales específicas de un país, cuando existan. No tienen la intención de rebajar el estándar establecido en esta Política. Estas variaciones específicas, junto con esta Política, pretenden asegurar que todo el personal entienda la obligación de la Empresa de cumplir con la legislación de protección de datos personales de todos los países en los que Nae opera.

Existen diferentes protocolos y procedimientos para ayudar al personal de Nae a interpretar y actuar de acuerdo con esta Política. Las directrices globales internas se documentarán en la herramienta de gestión documental de Nae (SharePoint.com/documentación interna) bajo la denominación "Global RGPD".

2. Nae procesa datos personales sobre los interesados, tales como su información personal (pasada y presente), solicitantes de empleo, contactos con clientes, contactos con proveedores, usuarios del sitio web y otras partes interesadas. Nae trata estos datos personales para desarrollar su actividad comercial, incluyendo:

   - Adquisición de talento.
   - Gestión del rendimiento de los empleados y su desarrollo profesional.
   - Nómina, control de gastos y contabilidad.
   - Gestión de relaciones comerciales con clientes y proveedores.
   - Promoción de la Empresa.
   - Infraestructura tecnológica y gestión de apoyo e instalaciones.
   - Otros fines exigidos por ley o reglamento.

b. Obligaciones de Nae

1. Para garantizar nuestro compromiso de cumplimiento normativo con el actual RGPD, únicamente trataremos datos personales de forma responsable, transparente y lícita. En particular, no trataremos datos a menos que alguna de las siguientes condiciones se cumplan:

   - Exista *consentimiento* otorgado por el interesado para tratar sus datos personales cuando la finalidad así lo requiera.
   - Para la *ejecución de un contrato* con el interesado o *cumplimiento de una obligación legal* de Nae.
   - Cuando sea necesario para la satisfacción de los *intereses legítimos* perseguidos por Nae, siempre que dichos intereses no prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado.

2. **Cuando se faciliten datos personales a Nae por parte de un interesado**, esta proporcionará desde el inicio información suficiente y clara a aquel acerca del tratamiento que se va a realizar, la identidad de la entidad de la Empresa que recoge/recibe datos personales, para qué va a utilizar esos datos y su finalidad. En particular, la información básica que recibirá el interesado incluirá el nombre de la Empresa (o en su caso, el de su filial o subsidiaria), el uso previsto de esos datos, la condición bajo la cual se tratan, el tipo de datos personales que son necesarios y cualquier información adicional que Nae considere necesaria para tratar los datos de forma leal, transparente y lícita. Por ejemplo, información sobre los destinatarios de los datos, sus derechos en virtud de la presente Política y normativa vigente, los plazos de conservación, la posibilidad de realizar transferencias internacionales, y las medidas técnicas y organizativas que aplicamos para mantenerlos confidenciales, íntegros y disponibles.

Cuando se proyecte un tratamiento para un fin distinto del que se recogieron, Nae se asegurará de proporcionar información al interesado sobre ese otro fin y cualquier información pertinente de acuerdo con lo indicado anteriormente.

3. **En el caso de la recogida indirecta de datos personales sobre un interesado** (por ejemplo, de un tercero, como una agencia de contratación, referencias, etc.), Nae informará al interesado de la identidad de la entidad de la Empresa que mantiene los datos y de lo que pretende hacer con ellos tan pronto como sea posible después de la recogida/recepción y/o decisión de conservar los datos. Nae proporcionará desde el inicio información suficiente y clara al interesado acerca del tratamiento que se va a realizar, la identidad de la Empresa que recoge/recibe datos personales, para qué va a utilizar esos datos y su finalidad. En particular, la información básica que recibirá el interesado incluirá el nombre de la empresa, el uso previsto de esos datos, la condición bajo la cual se tratan, el tipo de datos personales que son necesarios y cualquier información adicional que Nae considere necesaria para tratar los datos de forma leal, transparente y lícita. Por ejemplo, información sobre los destinatarios de los datos, sus derechos en virtud de la presente Política y normativa vigente, los plazos de conservación y la posibilidad de realizar transferencias internacionales, y las medidas técnicas y organizativas que aplicamos para mantenerlos confidenciales, íntegros y disponibles.
   Esta información no se facilitará al interesado cuando: (i) ya disponga de ella; (ii) la comunicación de dicha información resulte imposible o el esfuerzo implicado sea desproporcionado. A la hora de determinar lo que constituye o no un "esfuerzo desproporcionado", Nae debe sopesar la cantidad de esfuerzo requerido con la gravedad, si la hubiera, de un efecto perjudicial para la persona a la que se refieren los datos si no se le proporcionara dicha información.

4. Por lo general, Nae no necesita o pretende recoger información relacionada con las siguientes categorías de datos:

   - Origen racial o étnico;
   - Opiniones políticas;
   - Creencias religiosas, filosóficas u otras creencias similares;
   - Afiliación sindical;
   - Salud física o mental;
   - Datos genéticos o biométricos;
   - Orientación o vida sexual, y/o

- Condenas e infracciones penales o administrativas.

Nae no recogerá tales datos a menos que: (i) el interesado está de acuerdo prestando su consentimiento explícito para que Nae pueda hacerlo, basándose en una comprensión completa de por qué se están recogiendo estos datos, o (ii) Nae necesita hacerlo para cumplir con sus obligaciones o ejercer sus derechos en virtud de la legislación laboral, o (iii) en circunstancias excepcionales tales como cuando el tratamiento es necesario para proteger los intereses vitales del interesado, o (iv) en circunstancias permitidas por la legislación vigente de protección de datos personales.

Nae puede, en circunstancias excepcionales, confiar en el consentimiento dado en nombre del interesado, por ejemplo, por un empleado de la empresa en nombre de un miembro de la familia. El interesado deberá de ser informado por aquel en los mismos términos previstos en el punto (ii) de este apartado, y obtener su consentimiento para el tratamiento de sus datos, sin que Nae pueda asumir responsabilidad alguna por incumplimiento.

Como norma general, está totalmente prohibida la creación y mantenimiento de ficheros que almacenen categorías especiales de datos (datos sensibles que revelen información sobre salud, origen racial o étnico, vida u orientación sexual, ideología, afiliación sindical, convicciones religiosas o filosóficas, datos genéticos, datos biométricos, o aquellos que contengan información derivada de actos de violencia de género o antecedentes penales).

Se exceptúa de lo establecido con anterioridad al Servicio Médico, que podrá crear y mantener ficheros que contengan datos de carácter personal sobre salud, siempre y cuando exista el consentimiento explícito de los afectados y los datos sean tratados con la exclusiva finalidad de realizar las actividades propias de dicho Servicio, si existiera.

Asimismo, las áreas de Nae relacionadas con la gestión de los recursos humanos, básicamente, las Unidades de Relaciones Humanas, o de Administración de Personal, podrán crear y mantener ficheros que contengan datos de carácter personal sobre minusvalía y afiliación sindical, con la exclusiva finalidad de gestionar obligaciones legales, como, por ejemplo, la gestión de nóminas e impuestos.

Adicionalmente, en el caso de disponer de información sensible sobre salud, origen racial o étnico, vida u orientación sexual, ideología, afiliación sindical, religión o creencias, además de las excepciones ya comentadas, ésta será autorizada cuando se cumplan las siguientes premisas:

a) Cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de los que los interesados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

5. La Empresa dispondrá de procedimientos y protocolos para verificar que:

   - no recoge datos personales excesivos;
   - los datos personales recogidos son adecuados y pertinentes para los fines previstos, exactos y actualizados;
   - procesa datos personales sólo para los fines especificados en esta Política o en la información facilitada al interesado; y
   - se cumple una de las condiciones del apartado III.b.1., si trata datos personales para fines nuevos o diferentes.

6. Nae aplicará las políticas y procedimientos de conservación de datos personales, de modo que aquellos se eliminen después de un tiempo

razonable, en función de las finalidades para las que se mantienen los datos personales, excepto en los casos en los que, dadas esas finalidades, la legislación aplicable exija que se conserven los datos durante un cierto periodo de tiempo. Cuando ya no necesite conservar los datos personales para los fines para los que se obtuvieron, se destruirán siguiendo los protocolos internos de Nae.

7. Nae mantendrá las medidas de seguridad técnicas, organizativas y físicas en relación con todos los datos personales que trate. Velará por que dichas medidas sean adecuadas a los riesgos que entraña el tratamiento y a la naturaleza de los datos personales. Las medidas a aplicar por Nae serán, como mínimo, aquellas indicadas en el apartado de medidas de seguridad de esta Política.

   Cuando proceda, estas medidas deberán de exigirse, de acuerdo con los riesgos existentes en cada caso, a los proveedores de servicios externos con acceso a datos personales, considerando especialmente la tipología de datos, las categorías de interesados, destinatarios y tecnologías utilizadas para el tratamiento. Nae es consciente, en particular, de que es importante tomar medidas de seguridad adecuadas cuando se trata de que los proveedores de servicios externos (también conocidos como "encargados de tratamiento") traten datos personales en nombre y por cuenta de la Empresa, eligiendo solo aquellos que garanticen el cumplimiento con la legislación vigente de protección de datos personales. Nae se asegurará de que los proveedores de servicios están obligados por contratos escritos por medio de los cuales acepten tratar dichos datos sólo bajo las instrucciones de Nae y aplicar todas las medidas de seguridad apropiadas para proteger dichos datos. Cuando los proveedores de servicios estén localizados en países fuera de la UE y tengan acceso o traten datos personales procedentes de entidades de Nae en la UE, los contratos con dichos proveedores de servicios incluirán las cláusulas tipo normalizadas y aprobadas por la Comisión Europea (de responsable a encargado).

8. Nae reconoce que los datos personales deben ser tratados con cuidado en países en donde no existen leyes de protección de datos, o cuyas leyes de protección de datos no proporcionan un nivel de protección adecuado al estándar dentro de la UE. Nae no transferirá datos personales a entidades ajenas a la Empresa en dichos países para su posterior tratamiento (excepto para el tratamiento en nombre y por cuenta de la Empresa), a menos que dichas entidades acuerden cumplir con un estándar de protección de datos al menos tan alto como esta Política, o celebrar un contrato que incluya las cláusulas tipo aprobadas de la UE para las transferencias de datos personales a países fuera de la UE.

   Las únicas excepciones aplicables serán:

   (i) Cuando la transferencia es necesaria para:

   a) proteger los intereses vitales del interesado en una situación de "vida o muerte", o

   b) Celebrar o ejecutar un contrato con (o en beneficio de) el interesado;

   (ii) El interesado ha consentido la transferencia.

9. Nae cuenta con protocolos para gestionar cualquier sospecha de incumplimiento de las medidas de seguridad de los datos personales, acceso o divulgación no autorizados y eliminación o pérdida de estos. En particular, Nae dispone de procedimientos para registrar y notificar, tanto a la autoridad de control correspondiente como a los interesados, en su caso, sobre una violación de la seguridad de los datos personales, cuando dicha notificación sea legalmente obligatoria, o cuando Nae lo considere apropiado. En el caso de que ocurra este evento, los empleados deben seguir las instrucciones previstas en el protocolo de notificación y registro de violaciones de seguridad de datos de Nae.

IV. Derechos del interesado

a. Derecho de acceso

A petición escrita de un interesado, y cuando Nae tenga o reciba suficiente información para identificarlo y compruebe si tiene datos personales de aquel, se procederá de la siguiente manera:

1. Informará al interesado si Nae posee datos personales de aquel;
2. Informará sobre los datos personales que obran en su poder, el motivo de su conservación y los destinatarios a los que puede revelar aquellos; y
3. Proporcionará al interesado copias de los datos personales que obran en su poder, indicando el origen de los datos, si se conoce.

Nae proporcionará esta información y copias dentro de un plazo razonable después de la solicitud de ejercicio del derecho por el interesado, y en cualquier caso dentro del término máximo de 1 mes. Si la solicitud se ha realizado por medios electrónicos, la información se facilitará en un formato electrónico de uso común, a menos que el interesado la solicite de otro modo.

No obstante, Nae puede negarse a proporcionar información a un interesado cuando el acceso a esa información revelaría información sobre otro individuo (en cuyo caso Nae proporcionará tanta información como sea posible sin revelar información sobre el otro individuo), a menos que el otro individuo esté de acuerdo en que Nae pueda revelar la información o Nae decida que es razonable proporcionar la información sin el consentimiento del otro individuo.

Asimismo, en algunos países pueden existir otras razones legítimas para denegar la solicitud de acceso de un interesado, de conformidad con la legislación local de protección de datos.

b. Derecho de rectificación

Un interesado puede solicitar a Nae la rectificación de los datos personales que tiene sobre aquel. Si Nae considera que los datos son incorrectos, los borrará o corregirá. Si no está de acuerdo con que los datos sean incorrectos, registrará, no obstante, en el fichero o ficheros correspondientes el hecho de que el interesado considera que los datos son incorrectos.

En casos de rectificación, el interesado deberá:

1. Indicar en su solicitud a qué datos se refiere, y la corrección que haya de realizarse.

2. La documentación justificativa de la inexactitud o carácter incompleto de los datos, cuando así sea preciso.

c. Derecho de supresión

Nae suprimirá y dejará de tratar los datos personales a petición de un interesado cuando concurra alguna de las siguientes circunstancias:

- Dejen de ser necesarios para los fines que fueron recabados.
- Se haya retirado el consentimiento por el interesado y el tratamiento no se base en otra condición.
- El interesado se opone al tratamiento de los sus datos conforme a una solicitud de oposición.
- Los datos han sido tratados ilícitamente.
- Para el cumplimiento de una obligación establecida por ley.

La supresión, si procede, dará lugar al **bloqueo** de los datos personales, conservándose únicamente a disposición de jueces y tribunales y las Administraciones públicas competentes, en especial, la autoridad de control de protección de datos, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la eliminación.

d. Derecho de oposición

i. A promoción y venta directa

Nae acatará cualquier solicitud de un interesado de no utilizar sus datos personales con fines de marketing directo y lo hará de forma gratuita para el interesado.

ii. Por motivos relacionados con la situación particular del interesado

Cuando Nae se base en la condición del consentimiento o de intereses legítimos, indicadas en III.b.1 de estas Políticas, para justificar el tratamiento de datos personales, Nae acatará cualquier solicitud justificada de un interesado para que cese el tratamiento de sus datos si aquel se opone al tratamiento sobre la base de cualquiera de estas condiciones.

Sin embargo, en el caso de no darse curso a la solicitud, Nae deberá de acreditar motivos legítimos imperiosos para seguir con el tratamiento que prevalezcan sobre los intereses y derechos del interesado o bien para la formulación o defensa de reclamaciones.

La posibilidad del ejercido del derecho de oposición para fines de marketing directo debe ser comunicado explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

e. Derecho en relación con la toma de decisiones automatizadas

Por lo general, Nae no tomará decisiones que afecten significativamente a un interesado basándose únicamente en el tratamiento automatizado de datos que evalúen aspectos personales del interesado (como su rendimiento en el trabajo, solvencia, fiabilidad o conducta). Cuando Nae utilice alguna vez dichas técnicas de toma de decisiones en el curso de la celebración o ejecución de un contrato con el interesado, o cuando dicha

técnica de toma de decisiones esté autorizada por ley, se asegurará de que se implementen las medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado. Los interesados tienen derecho a recibir una explicación clara del método y los criterios utilizados para tomar cualquier decisión basada en la toma de decisiones automatizadas.

f. Derecho a la limitación del tratamiento

La limitación al tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Se puede solicitar la limitación cuando:

a. El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
b. El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
c. Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

g. Derecho de portabilidad

El derecho a la portabilidad de los datos es el derecho del interesado a recibir los datos personales que le incumban. Es una forma avanzada del derecho de acceso, por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica.

Este derecho sólo puede ejercerse:

a. Cuando el tratamiento se efectúe por medios automatizados.
b. Cuando el tratamiento se base en el consentimiento o en un contrato.
c. Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

El derecho a la portabilidad implica que los datos personales del interesado se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible

h. Derechos conforme a la normativa de protección de datos vigente

Los derechos enunciados en esta sección se entienden sin perjuicio de los derechos que pueda tener un interesado en virtud de la legislación aplicable en protección de datos personales a presentar una reclamación ante la autoridad nacional de control de protección de datos o a reclamar una indemnización por infracción de la legislación aplicable en esta materia.

V. Notificaciones de incidentes de seguridad

Nae dispone de un procedimiento de notificación, gestión y respuesta frente a cualquier anomalía o incidente de seguridad, especialmente aquel que afecte o pueda afectar a la seguridad de los datos, adaptado a las nuevas exigencias de la normativa de protección de datos.

Nae contará con el apoyo de un Responsable de seguridad para la gestión de cualquier incidente de seguridad y aquellos que impliquen un riesgo para los derechos y libertades de los interesados. La identificación y funciones del Responsable de seguridad se encuentran documentadas en las directrices de aplicación de estas Políticas.

a. Notificaciones

1. Interna

- Cualquier persona que forme parte de la plantilla de la Empresa o se halle prestando sus servicios temporalmente en la misma, así como cualquier encargado de tratamiento, deberá notificar inmediatamente al departamento o cargo designado en Nae como punto inicial de contacto para estos asuntos, cualquier anomalía que detecte y especialmente aquella que afecte o pueda afectar a la seguridad de los datos. El departamento o cargo designado se encargará, en su caso, de comunicar inmediatamente al Responsable de seguridad del incidente.
- Ante los graves perjuicios que se pueden ocasionar, Nae actuará disciplinariamente en el supuesto de no actuar con la máxima diligencia ante una irregularidad en el funcionamiento habitual del sistema informático.
- El procedimiento de notificación se realizará a mediante la herramienta Zendesk, de acuerdo con lo establecido en los procedimientos internos del área IT de Nae.

2. Externa

2.1. Notificación a la Agencia Española de Protección de Datos

- Nae notificará a la autoridad de control competente sin dilación indebida las anomalías o violaciones de la seguridad de los datos personales, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas interesadas.

2.2. Notificación a los interesados

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de los interesados, Nae se las comunicará sin dilación indebida.
- No obstante, la comunicación al interesado no será necesaria si Nae ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad (en particular el cifrado), o que estas medidas garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado o que dicha comunicación suponga un esfuerzo

desproporcionado. En este último caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

b. Gestión

1. Interna

- El Responsable de seguridad elaborará y/o recibirá las notificaciones de incidencias y procederá a su registro y análisis. En su caso, comunicará dicha incidencia a los técnicos internos o externos encargados de la seguridad del sistema.
- El Responsable de seguridad se asegurará de que los técnicos, en su caso, den respuesta inmediata a la incidencia detectada y supervisará el trabajo de subsanación de la anomalía detectada. Una vez finalizada la subsanación, enviará un informe a la dirección de Nae, con todos los datos requeridos para el registro de la incidencia.

2. Externa

2.1. Agencia Española de Protección de Datos

- La notificación a la autoridad de control contemplada en el apartado anterior deberá de realizarse a más tardar 72 horas después de que haya tenido constancia de la violación de la seguridad de los datos personales.
- La comunicación a la autoridad de control sólo tendrá lugar cuando exista una violación de seguridad en los datos personales, no cualquier incidente de seguridad, a saber:
    - Cuando exista destrucción, pérdida o alteración accidental o ilícita de datos personales.
    - Cuando exista comunicación o acceso no autorizado de datos personales.
- En caso de que, previa evaluación del riesgo del incidente y de las medidas de seguridad aplicadas antes, durante y después del incidente, dicha notificación sea necesaria por cumplirse lo indicado en el aparatado anterior, aquella deberá contener, como mínimo:
    i. Tipo de incidencia, anomalía o violación de la seguridad de los datos personales. Una descripción de esta e inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
    ii. Momento en el cual se ha producido la incidencia.
    iii. El nombre y los datos de contacto del responsable de seguridad, del delegado de protección de datos en su caso, o de otro punto de contacto en el que pueda obtenerse más información.
    iv. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
    v. Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos del retraso.

2.2. Interesados

- La comunicación al interesado contemplada en el apartado anterior deberá describir en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas indicadas para las notificaciones a la autoridad de control, descritas anteriormente.

c. Registro y documentación

- Nae deberá documentar cualquier incidente de seguridad y violación de la seguridad de los datos personales y crear un registro en el cual se haga constar la siguiente información:
    i. Tipo de incidencia, anomalía o violación de la seguridad de los datos personales.
    ii. Momento en el cual se ha producido.
    iii. Persona que realiza la notificación y la gestión externa de las comunicaciones.
    iv. Efectos derivados de dicha notificación.
    v. Consecuencias de la violación de la seguridad de los datos.
    vi. Descripción de las medidas correctivas adoptadas o propuestas.
- El registro de incidencias se mantendrá actualizado en todo momento.
- Es obligación del responsable del sistema gestionar las incidencias que pudieran producirse, en el menor tiempo posible, garantizando, en todo caso, que la seguridad de los datos de carácter personal no se vea alterada en ningún momento.
- La ficha para el registro y documentación de un incidente de seguridad y la violación de seguridad sobre datos personales se incluye en el documento de aplicación y cumplimiento de esta Política.

d. Encargados de tratamientos

- Cuando la violación de seguridad se produzca en el proveedor de servicios externos y afecte datos personales de Nae, aquel deberá de notificar a Nae, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de correo electrónico o teléfono, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, conjuntamente con toda la información relevante para la documentación y comunicación de la incidencia.
- La información a facilitar, en caso de disponerse de aquella, será la siguiente, como mínimo:
    i. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
    ii. El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto del Encargado en el que pueda obtenerse más información.
    iii. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
    iv. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

- A petición de Nae, el Encargado realizará o dará apoyo a éste en la realización de las comunicaciones de las violaciones de la seguridad de los datos personales a la autoridad de protección de datos y a los interesados, en caso de que corresponda. Se establecerán estas obligaciones por contrato escrito y el encargado del tratamiento no difundirá ni llevará a cabo ninguna comunicación o aviso, sobre cualquier incidente de seguridad en los datos, en relación con la prestación del servicio objeto de este contrato, sin la aprobación previa de Nae.
- La ficha para el registro y documentación de la violación de seguridad sobre datos personales se incluye en el documento de aplicación y cumplimiento de estas Políticas.

VI. Medidas de seguridad a aplicar en la organización

En Nae el tratamiento de datos personales se realiza a través de procedimientos automatizados (electrónicos) y no automatizados (papel). Para todos ellos, deben de tenerse en consideración los riesgos existentes, cuya materialización repercutirá en mayor o menor medida despendiendo de la probabilidad e impacto de las amenazas inherentes que apliquen a cada uno de ellos (incumplimiento normativo, confidencialidad, integridad y disponibilidad de la información y datos personales), y que los cuales se pretenden mitigar garantizando la aplicación de las diferentes medidas de seguridad que a continuación se detallan.

Tratamientos automatizados

Organización de la Seguridad

- Establecimiento de unas políticas transparentes y claras de protección de datos de acuerdo con la normativa vigente, comunicadas y aceptadas por todos los empleados, proveedores y terceras partes.
- Campañas de concienciación y formación en protección de datos y seguridad de la información para todos los usuarios que tengan acceso a datos personales.
- Contar con una estructura interna (departamento, responsable o comité) encargada de que la organización y todo su personal cumpla con la normativa de protección de datos personales.
- Incorporación en los contratos de trabajo de las cláusulas de información, Políticas de protección de datos y Normas de uso y seguridad de la Información en el uso de los recursos y sistemas informáticos de la organización. Toda la documentación debe ser aceptada y firmada por el empleado previa concesión de acceso a cualquier activo en donde se trate datos personales.
- Cualquier empleado que tenga acceso a datos personales deberá recibir un curso de formación específico y adecuado para las funciones que desarrolla.
- Elaboración de un inventario de recursos TIC (servidores locales y virtuales, hardware, software, BBDD, discos duros, pendrives, routers, aplicaciones) que contengan y procesen datos personales y procedimientos de actualización periódicos.

- Elaboración de un registro con la asignación de propietario de cada activo del inventario, autorizaciones, nivel de criticidad y responsabilidades.

Control de acceso físico e instalaciones

- Mecanismos perimetrales de seguridad física en las instalaciones donde se traten datos personales (despachos, salas de servidores/centros de proceso de datos (CPD), archivos), sistemas de detección de intrusos, a fin de evitar accesos y/o modificaciones de los sistemas y recursos que contengan datos personales.
- Mecanismos para el registro de acceso físico a instalaciones en donde se procesan datos personales y medidas de control técnicas y organizativas para el acceso (sistemas de control electrónico, tarjeta, llave, sistema de alarma, sensores de presencia, identificación del personal).
- El acceso a zonas restringidas o de seguridad (por ejemplo, CPD) deberán de estar autorizadas expresamente y contar con medidas de control de acceso y videovigilancia que aseguren que únicamente personal autorizado accede a aquellas.

Control de acceso lógico

- Definición de procedimientos para la gestión de cuentas de usuarios: registro, alta, modificación y baja/revocación de usuarios con acceso a sistemas o aplicaciones informáticas que procesen datos personales.
- Designación de identificador unívoco a cada usuario para el acceso.
- Registro de identificadores, con los privilegios asociados respectivos, en función del cargo y las funciones del usuario que solicita el acceso. En función de dichos privilegios, el usuario podrá acceder únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones.
- Los identificadores y claves de acceso asignadas a cada usuario son personales e intransferibles. Está expresamente prohibido compartir o facilitar el identificador de usuario y la clave de acceso a los sistemas y recursos TIC de Nae a otra persona física o jurídica, incluido el personal de la propia empresa, así como también a utilizar las contraseñas de otros usuarios.
- En el caso de que la longitud de la lista o la frecuencia de las actualizaciones sean muy altas, dicho registro se remitirá a la relación de usuarios que se encuentra en cada servidor o aplicación en formato digital.
- Disponer de procedimientos de revisión periódica de permisos en los recursos y sistemas TIC.
- Disponer de un registro/log de accesos a aplicaciones y sistemas: intentos de acceso exitosos y fallidos, acceso con perfil de administrador, creación, modificación o eliminación de datos personales efectuados. Dicho registro deberá permitir identificar como mínimo quien ha realizado la acción, cuando se ha llevado a cabo y el tipo de actividad realizada (p.ej. inicio de sesión, modificación de registro, intento fallido, bloqueo de cuenta).

- Disponer de mecanismos para la revisión periódica de accesos en sistemas o aplicaciones.
- Los datos de registro/logs deben almacenarse de forma segura y su acceso está reservado a personal autorizado.
- Todos los cambios (altas, modificación, baja) en cuentas de usuarios deberán de ser trazables y estar documentados.
- Cuando finalice la relación contractual, la autorización de acceso a usuarios debe ser revocada de forma inmediata.
- Cuando se produzca una ausencia temporal (p.ej. vacaciones, baja médica) y sea necesario el acceso a la cuenta del usuario ausente, se deberá de conceder autorización previa de acceso.

Contraseñas

- La asignación y distribución de contraseñas se hará a través del sistema, de forma automática, garantizando su confidencialidad e integridad.
- La contraseña debe cambiarse de forma obligatoria tras el ingreso de la contraseña por defecto facilitada al inicio para el acceso a los sistemas donde se procesen datos personales.
- En la gestión y uso de las contraseñas se establecerán como mínimo las siguientes pautas de seguridad:
    a. La contraseña debe tener una extensión mínima de seis caracteres alfanuméricos (números, letras y caracteres especiales).
    b. No se deben utilizar palabras comunes, fechas de aniversario, matrículas de coche, etc.
    c. Se deben crear nuevas contraseñas y evitar reutilizar las contraseñas antiguas.
    d. Se deben cambiar las contraseñas regularmente, y como mínimo una vez cada 6 meses. El sistema deberá forzar el cambio transcurrido el plazo de validez máximo de 6 meses.
    e. Al recibir soporte técnico, los usuarios tendrán que introducir personalmente todas las contraseñas.
    f. No se debe facilitar la contraseña a los empleados de servicios externos de asistencia técnica.
    g. No se deben conservar las contraseñas en papel.
    h. Las contraseñas almacenadas en los sistemas deberán estar cifradas.
    i. Debe impedirse la visualización de la contraseña durante su introducción.
    j. El número de intentos fallidos consecutivos al momento de introducir la contraseña antes de que la cuenta se bloquee debe ser, como máximo, 3 veces.
- Disponer de mecanismos automáticos de bloqueo de pantallas con contraseña por inactividad superior a, como máximo, 10 minutos.

Resiliencia operacional

Copias de seguridad

- Disponer de un procedimiento de realización de copias de respaldo y recuperación de datos que garantiza su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, que establezca la frecuencia de respaldo, la ubicación física de las copias y las medidas para garantizar la confidencialidad e integridad de la información.
- Dicho procedimiento consiste en la realización, con periodicidad diaria, de una copia de respaldo de la información de la organización en el servidor virtual, previamente configurado.
- En el caso de producirse una incidencia que genere destrucción de información, se aplicará el procedimiento de notificación, tratamiento y registro de incidencias previsto en el manual de protección de datos, y se procederá a la recuperación de la información destruida. Si dicha recuperación fuese imposible, se procederá a solicitar la copia de respaldo más reciente y a restaurar la información destruida.
- Cifrado de datos en las copias de seguridad.

Planes de continuidad del negocio

- Disponer de un plan de continuidad documentado, sobre los sistemas y recursos informáticos donde se procesan datos personales, procesos definidos, requisitos de seguridad, organización.
- Pruebas del plan de continuidad de negocio o recuperación de desastres: informes de implementación y revisión.

Protección de activos

- Disponer de herramientas y sistemas antimalware actualizados (antivirus, cortafuegos, IPS, etc.).
- Sistemas/aplicaciones con los últimos parches o actualizaciones instaladas. Sistemas/aplicaciones con vulnerabilidades mitigadas.
- Implantación de sistemas y controles de detección de incendios, inundaciones, humedad, corte de suministro eléctrico, para proteger los activos que procesan datos personales de amenazas del entorno y asegurar la disponibilidad de la información.
- Implantación de revisiones o pruebas periódicas de los mecanismos de detección de amenazas del entorno.
- Procedimientos establecidos de gestión de autorizaciones para la salida de soportes de almacenamiento de datos fuera de las instalaciones de la organización.
- Los portátiles deben asegurarse con un cable de seguridad, siempre que sea posible, en cualquier lugar en el que se utilicen, y deberían guardarse en un armario bajo llave durante la noche o cuando no se usen durante un periodo prolongado de tiempo.
- Los portátiles y todos los dispositivos móviles en general no deben guardarse ni siquiera de forma temporal en un coche o en un lugar de acceso público.

- Debe informarse de inmediato sobre cualquier robo o pérdida de hardware. En caso de robo o pérdida de un ordenador o cualquier otro dispositivo móvil, deberá notificarse de inmediato al departamento o persona responsable designada.
- Cifrado de las BBDD, discos duros en equipos y/o del ambiente de producción del sistema.
- Documentación de políticas internas de uso de recursos y sistemas que tratan datos personales debidamente notificadas.
- Los soportes magnéticos que vayan a ser reutilizados o desechados deberán ser previamente desmagnetizados con el fin de efectuar un borrado total de los datos.
- Alternativamente, podrán utilizarse otros sistemas que garanticen que los datos no podrán ser recuperados en ningún caso. Procedimientos de formateo de la información en equipos reutilizables.

Comunicaciones y almacenamiento

- Sistemas de monitorización y registro de eventos en las comunicaciones, conforme a las normas de uso de sistemas y recursos TIC.
- Cifrado de las comunicaciones y/o la información saliente que contenga datos personales de un sistema, en particular aquellas con datos sensibles.
- La transmisión mediante soportes físicos de datos personales deberá estar autorizada, y constar una lista de registro indicando persona responsable, fecha, tipo de datos y soporte, destinatario y medidas técnicas y organizativas para garantizar la confidencialidad de la información.
- Para limitar al máximo el riesgo de pérdida de información confidencial, es obligatorio guardar los documentos informáticos en el servidor y no conservar ninguno en el disco duro de los ordenadores personales. Por el mismo motivo se prohíbe el uso de soportes, pen drive, discos duros portátiles y cualquier otro dispositivo móvil que pueda almacenar información. Sólo podrán utilizarse los dispositivos móviles expresamente autorizados e inventariados por el responsable de seguridad.
- En caso de que un usuario sea autorizado para realizar conexión remota o teletrabajo, se deberán establecer canales de comunicación seguros (SSH, VPN, TLS/SSL, etc.) y se deberá aplicar medidas adicionales de seguridad en el lugar donde se encuentre ubicado el equipo, para garantizar un nivel de confidencialidad similar al de las instalaciones de la organización.
- En su caso, las mismas cautelas deberán aplicar los usuarios que accedan a los servidores que procesan datos personales a través de la VPN o de cualquier otro sistema de conexión remota, ya que durante la conexión se incrementa el nivel de vulnerabilidad del sistema.

Ficheros temporales

A los efectos de este documento, se consideran ficheros temporales los ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

- Los ficheros temporales y las copias de documentos que se hayan creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.
- Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- Los ficheros temporales creados de forma automática por las aplicaciones deberán ser eliminados también de forma automática por las propias aplicaciones al finalizar la sesión.
- Los ficheros temporales generados por los sistemas operativos deberán ser eliminados periódicamente como consecuencia de los procesos automáticos de los propios sistemas operativos, en función de la configuración de estos, o de forma manual, cuando ello sea necesario.

Régimen de contratación de servicios externos

- Existencia de cláusulas relativas a la seguridad de la información y protección de datos en los contratos celebrados con proveedores externos con acceso a datos personales.
- Celebración de acuerdos de confidencialidad con proveedores externos con acceso a las instalaciones de la organización, que no tengan acceso a datos personales (p.ej. limpieza, revisión de extintores, maquinaria, etc.).
- Disponer de procedimientos de selección de proveedores que garanticen el cumplimiento de la normativa de protección de datos. Se deberán de establecer criterios de selección teniendo en cuenta el nivel de criticidad de los datos personales tratados, tecnologías utilizadas y destinatarios de los datos.
- Disponer, documentar y almacenar aquellas evidencias de cumplimiento con el RGPD aportadas por proveedores de servicios (certificaciones, adhesión a códigos de conducta, registro de actividades, informes de análisis de riesgos o PIAs).

Gestión de soportes

- Disponer de una relación detallada de los soportes homologados existentes dentro de la organización que procesen datos personales.
- Mecanismos de actualización de dicha relación, mediante inventarios periódicos.
- Autorizaciones para salidas de soportes fuera de las instalaciones de la organización, documentadas (datos del peticionario, soporte y finalidad).
- Sistema de registro de salida de soportes.
- Cifrado de soportes donde se procesen datos personales, en especial medida aquellos soportes portátiles (móviles, USB, portátiles, tablet).

Gestión de incidentes de seguridad

- Existencia de un procedimiento definido para la notificación interna y externa de incidentes que impacten en la seguridad de los sistemas y recursos que traten datos personales. Dicho procedimiento será descrito en la Política de protección de datos y su documento de aplicación y cumplimiento, y comunicado a todas las personas con acceso a sistemas y recursos TIC de la organización, así como también a los proveedores externos que por razón del encargo de servicios tengan acceso a datos personales.
- Disponer de herramientas de detección y protección frente a software dañino (virus, troyanos, ransonware, etc.) lo suficientemente robustas de acuerdo con el arte vigente.

Controles periódicos

- De forma continuada y con una frecuencia mínima de una vez al año, se llevarán a cabo los controles periódicos que se deben realizar para verificar el cumplimiento de las medidas y controles de seguridad.
- Los controles periódicos actuarán en las siguientes áreas:
  - Control de la aplicación del plan de seguridad.
  - Control del sistema de identificación y autenticación.
  - Control del sistema de control de acceso lógico y físico.
  - Control del cumplimiento de las normas de confidencialidad y secreto.
  - Control del cumplimiento de las normas internas y las funciones del personal.
  - Control de los procedimientos de gestión de soportes.
  - Control antivirus.
  - Control del cumplimiento de las normas de propiedad intelectual

Tratamientos no automatizados

El objetivo final de la organización es aplicar el principio de “oficina sin papeles” por motivos de seguridad, de espacio y por razones ecológicas. Ello significa que, en la medida de lo posible, todas las áreas de negocio deberán utilizar un sistema informático de gestión documental que sustituya progresivamente el papel, escaneando los documentos para conservarlos en formato digital.

No obstante, deben considerarse las siguientes excepciones, en el caso de que puedan ser de aplicación:

- Documentos que se gestionan en papel por cuestiones de agilidad (partes de baja).
- Documentos que tradicionalmente se conservan en formato papel (TC1; TC2; CV).
- Documentos originales con fuerza probatoria (Contratos, actas, escrituras).

Criterios de archivo

- El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación.
- En aquellos casos en los que no exista norma aplicable, se seguirán los criterios y procedimientos de actuación establecidos internamente en la organización (consentimiento RGPD, currículums).

Zonas de archivo

- En la zona de trabajo existen tres tipos de zonas de archivo:
    1. Las zonas de archivo inmediato, que contienen documentos activos y que se hallan próximas a las áreas de trabajo para facilitar las labores de archivo y consulta.
    2. Las zonas de archivo histórico que contienen documentos no activos y que se hallan en archivadores y armarios con llave, localizados en el mismo local de trabajo de la organización.
    3. Las zonas de archivo histórico que contienen documentos no activos y que se hallan localizados en las premisas del proveedor externo contratado para dicho fin, aplicando las medidas de seguridad y control establecidas en el contrato celebrado y en la normativa de protección de datos.
- Las zonas de archivo en donde se guarden datos sensibles (p.ej. ideología política, datos de salud, creencias religiosas, orientación sexual, delitos y condenas, etc.) deberán contar con suficientes controles perimetrales de acceso (p.ej. puertas dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente) que permitan que sólo tenga acceso el personal autorizado.

Dispositivos de almacenamiento

- Los dispositivos de almacenamiento de los documentos que contengan datos personales (p.ej. armarios, archivadores) deberán disponer de mecanismos que obstaculicen su apertura.

Custodia de los soportes

- Mientras la documentación con datos personales no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre a cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser objeto de acceso por persona no autorizada.
- Los armarios, archivadores u otros elementos en los que se almacenen los documentos con datos personales deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.
- En caso de traslado físico de la documentación fuera de las instalaciones de la organización, se deberá impedir en todo momento el acceso no autorizado o manipulación de la información por parte de personal no autorizado.
- Se deberá asignar plazos de conservación específicos para la documentación en formato papel de acuerdo con la legislación aplicable o, en su defecto, el

criterio aplicado para su conservación cuando aquel no sea posible determinarlo o no venga impuesto por imperativo legal.

Destrucción y reutilización de soportes

- En el caso de los documentos en papel, la destrucción deberá realizarse de manera que el tamaño final del residuo impida acceder a los datos que contenía el documento. Para ello se podrán utilizar destructoras adecuadas o se contratarán los servicios de una empresa de destrucción confidencial de documentos, la cual deberá certificar la destrucción y permitir auditorías para su comprobación.

Autorizaciones

- La salida de soportes que contengan datos de carácter personal deberá de estar autorizada.
- Para el acceso a documentos que contengan datos sensibles (ideología política, datos de salud, creencias religiosas, orientación sexual, delitos y condenas, etc.) se deberá de contar con autorización previa, debidamente registrada.

VII. Cumplimiento de la Política

La Empresa mantendrá medidas internas para:

a) facilitar el cumplimiento de esta Política, tal y como se describe en el documento de *Aplicación y cumplimiento de la Política de Protección de Datos de Nae*

b) permitir el ejercicio efectivo de los derechos de los interesados, garantizados en la Política, según se describe en el documento de *Procedimientos para responder a las solicitudes de ejercicio de derechos de los interesados*;

c) cumplir con el deber de diligencia y vigilancia debida en la contratación y prestación de servicios externos, colaboraciones y cualquier esquema de gestión que implique participación de terceros con acceso a datos personales titularidad de Nae previsto en el documento *Régimen de Contratación de Servicios Externos de Nae.*

Los interesados pueden apoyarse en estas medidas y procedimientos y/o ejercer sus derechos previstos en la Política poniéndose en contacto con su Responsable Local de Protección de Datos o el Delegado de Protección de Datos.

Si una entidad de Nae tiene conocimiento de la existencia de algún requisito bajo la legislación local que pudiera tener un efecto adverso sustancial en su capacidad para cumplir con esta Política (o que pudiera tener tal efecto si los requisitos no se impusieran a la entidad de la Empresa por ley), informará al Delegado de Protección de Datos y a la entidad (o entidades) de Nae cuyos datos procesa y cuyos datos se ven afectados por dicha legislación local.

VIII. Entidades de Nae actuando como Encargados de Tratamiento

Cuando una entidad de Nae procesa datos personales en nombre y por cuenta de otra entidad de Nae, la primera de ellas se denomina en esta Política "Encargado del Tratamiento" y la segunda "Responsable del Tratamiento".

El Encargado del Tratamiento deberá en todo momento observar lo siguiente:

1. Tratar los datos personales únicamente siguiendo las instrucciones del Responsable del Tratamiento;
2. Aplicar las medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción accidental o ilícita o la pérdida accidental, la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento implique la transmisión de datos a través de una red, y contra cualquier otra forma ilícita de tratamiento;
3. Hacer todos los esfuerzos razonables para mantener los datos personales de manera que sean exactos y estén actualizados en todo momento;
4. No revelar los datos personales a ninguna persona excepto en la medida en que lo exija o permita la ley o cualquier acuerdo entre el Responsable y el Encargado, o con el consentimiento por escrito del Responsable.
5. Proporcionar plena cooperación y asistencia al Responsable del Tratamiento para permitir que los interesados a los que se refieren los datos personales ejerzan cualquier derecho en virtud de esta Política y seguir los procedimientos internos establecidos para la atención, registro, notificación de aquellos.
6. No procesar los datos personales excepto en la medida razonablemente necesaria para llevar a cabo cualquier acuerdo entre el Responsable y el Encargado en relación con los datos personales.
7. Asistir al Responsable en las consultas a la autoridad de control, evaluaciones de impacto y notificaciones de violaciones de seguridad en los datos personales.
8. Solicitar autorización expresa del Responsable del Tratamiento para cualquier subcontratación que implique el acceso a los datos personales a los que se ha dado acceso o facilitado.
9. Destruir o devolver los datos personales y la documentación y aplicaciones en los que se encuentren según las instrucciones del Responsable.

Este apartado, constituye una instrucción escrita del Responsable al Encargado, para que tome las medidas necesarias en el tratamiento de los datos personales a los que acceda como:

i. razonablemente considere necesario el Encargado para la ejecución de cualquier acuerdo celebrado con el Responsable en relación con los datos personales; y
ii. sean coherentes con las obligaciones del Encargado del tratamiento en virtud de dicho acuerdo o de cualquier otra normativa aplicable.

INFORMACIÓN DE CONTACTO

Para cuestiones relacionadas con esta Política pueden contactar con el Delegado de Protección de Datos, o en su caso, con el Responsable Local de la Protección de Datos. Para asuntos globales de privacidad, por favor contacte a (info@nae.global)