Contrato de Tratamiento de Datos Personales

Contrato de tratamiento de datos personales para clientes finales de los servicios de NOMINALIA
INTERNET S.L.

I.	Preámbulo	2
1.	Definiciones	3
2.	Papeles en la Protección de Datos.....	5
3.	Obligaciones del Encargado del Tratamiento.....	6
4.	Obligaciones del Responsable del Tratamiento	7
5.	Autorización para el Sub - tratamiento.....	7
6.	Transferencia de Datos Personales e inclusión de Cláusulas – Tipo (si fuese aplicable)	8
7.	Cooperación y obligaciones de Registro	8
8.	Derechos del Titular de los Datos (Interesado)	9
9.	Devolución y Borrado de Datos	9
10.	Transmisiones	10
11.	Violación de datos personales	10
12.	Recuperacion de desastres y continuidad del negocio	11
13.	Mandato	11
	Anexo 1	12
	Anexo 2	14
	Anexo 3	20
	ACUERDO DE TRATAMIENTO DE DATOS PARA CLIENTES QUE SOLICITAN LOS SERVICIOS DE NOMINALIA EN NOMBRE DE TERCEROS	21
II.	Preámbulo	21
1.	Definiciones	22
2.	Papeles en la Protección de Datos.....	24
3.	Obligaciones del Sub - Encargado del Tratamiento	24
4.	Cooperación y obligaciones de Registro	25
5.	AUTORIZACION PARA EL TRATAMIENTO DE DATOS POR OTROS SUB – ENCARGADOS.....	25

6. Derechos del Titular de los Datos (Interesado)	26
7. Devolución y Borrado de Datos	26
8. Violación de datos personales	27
9. Recuperación de desastres y continuidad del negocio	28
Anexo 1	29
Anexo 2	30
Anexo 3	35

I. PREÁMBULO

Considerando:

A.

Las leyes de protección de datos vigentes permiten que cualquier Responsable del Tratamiento de Datos Personales nombre a una persona física o jurídica, administración pública o cualquier otra entidad o asociación para actuar como Encargado del Tratamiento, en nombre del Responsable, entre las entidades que mejor se adapten, en virtud de su experiencia, capacidades y fiabilidad, al cumplimiento de las Leyes de Protección de Datos que sean de aplicación, también en relación con los aspectos relacionados con la Seguridad.

B. El Encargado del Tratamiento designado debe dar suficientes garantías para implementar las medidas técnicas y organizativas apropiadas, de tal forma que el Tratamiento cumpla los requisitos de las Leyes de Protección de Datos personales y asegure la protección de los derechos de los titulares de los Datos.

C. Este Acuerdo de Tratamiento de Datos, junto con sus Anexos (en conjunto "DPA") se celebra entre el CLIENTE (en adelante, el **Cliente**), la persona física o jurídica que contrata el Servicio, como se define más adelante, y cuyos datos se indican también más adelante, y NOMINALIA INTERNET S.L. (**NOMINALIA**) en conjunto, las "Partes" y singularmente cada uno de ellos como la "Parte", con el fin de reflejar el acuerdo de las Partes con respecto al Tratamiento de los Datos Personales del Cliente, de conformidad con los requisitos de las Leyes de Protección de Datos aplicables.

D. NOMINALIA presta al Cliente EL/LOS SERVICIO/S ("**Servicio/s**") y, para proporcionar éstos de conformidad con las condiciones contractuales establecidas en la Orden de Servicio u Órdenes de Servicio y en las Condiciones Generales del Servicio, todas ellas disponibles en el enlace

<https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/>

(MSA) y, con el fin de prestar el citado Servicio conforme a este DPA, NOMINALIA puede procesar / tratar Datos Personales en nombre del Cliente.

E. Más concretamente, el objetivo o propósito del tratamiento de los datos personales del cliente en relación con el Servicio está descrito en el **Anexo 1**.

F. El Cliente reconoce que su uso del Servicio puede estar sometido a las Leyes de Protección de Datos de jurisdicciones que impongan determinados requisitos en relación con el tratamiento de cualquier clase de Datos Personales.

G. Las partes han suscrito este DPA con el fin de asegurar que cumplen con las Leyes de Protección de Datos aplicables y para establecer salvaguardas y procedimientos para el tratamiento conforme a la ley de los Datos Personales. El Cliente confirma que las estipulaciones contenidas en este DPA reflejan las obligaciones que las leyes de protección de datos aplicables imponen a NOMINALIA relativas al tratamiento de datos personales del Cliente para la prestación del Servicio. NOMINALIA se compromete a cumplir con las previsiones contenidas en el presente DPA.

Este Preámbulo forma parte integral de este DPA.

1. DEFINICIONES

Salvo que se diga otra cosa en este DPA, todos los términos con mayúsculas aquí empleados tendrán el significado que se les da en el MSA. En caso de conflicto o de incongruencia en términos de las salvaguardias de protección de datos entre el DPA y el MSA, este DPA prevalecerá.

“**Decisión de adecuación**” significa una decisión legalmente vinculante emitida por la Comisión Europea y que permite la transferencia de Datos Personales desde el Espacio Económico Europeo hacia un tercer país que ha sido considerado adecuado en términos de garantías de protección de datos personales.

“**Leyes Aplicables de Protección de Datos**” significa en los países miembros de la UE, el Reglamento y las leyes complementarios en materia de Protección de Datos en esos países, incluyendo cualquier guía y/o códigos de prácticas emitidos por la Autoridad de Supervisión correspondiente en la UE; y/o en países no miembros de la UE, cualquier ley de protección de los Datos Personales relativa a la salvaguardia y tratamiento conforme a ley de Datos Personales.

“**Cliente**”: significa el sujeto que ha contratado el Servicio.

“**Datos Personales del Cliente**” significa Datos Personales relativos a Titulares de Datos, tratados en aplicación del Servicio que presta el Encargado del Tratamiento al Cliente.

“Responsable del Tratamiento” en general significa la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determina el objeto y significado del tratamiento de datos personales. Para los fines de este DPA, el Responsable del Tratamiento es el Cliente.

“Exportador de Datos” tiene el significado dado en las Cláusulas – Tipo.

“Importador de Datos” tiene el significado dado en las Cláusulas – Tipo.

“Encargado del Tratamiento” significa en general la persona física o jurídica, autoridad pública, agencia u otro organismo que trata datos en nombre del Responsable. Para los fines de este DPA, el Encargado del Tratamiento es NOMINALIA.

“Titular de los Datos” o **“Interesado”** tiene el significado que se le da en el Reglamento.

“Derechos del Interesado” significa los derechos que se le reconocen al Interesado de conformidad con las leyes de Protección de Datos aplicables. En la medida en que el Reglamento es aplicable, “Derechos del Interesado” significa, por ejemplo, el derecho a pedir al Responsable del Tratamiento acceso, rectificación o supresión de los Datos o limitaciones al tratamiento relativas al Interesado o negarse al tratamiento así como pedir la portabilidad.

“DPA” significa este Acuerdo Global de Tratamiento de Datos junto con sus anexos 1, 2 Y 3.

“EEE” significa el Espacio Económico Europeo.

“UE” significa la Unión Europea.

“Lista de subencargados” significa la lista disponible enviando una solicitud por escrito a dpo@nominalia.com

“MSA” significa los términos y condiciones incluidos en la Orden de Servicio y en las Condiciones de Servicio relativas a la prestación del Servicio acordadas entre las Partes y disponible en el siguiente enlace: <https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/>

“Entidad No - EEE” significa cualquier entidad que actúa como Encargado del Tratamiento (o sub – encargado) que trata datos del Cliente, para la prestación del Servicio, en un país fuera del EEE o en un país que no ha recibido una Decisión de Adecuación.

“Datos Personales” significa cualquier información relacionada con una persona física identificada o identificable; una persona física identificable es aquella que puede identificarse, directa o indirectamente, en particular por referencia a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos de los factores físicos, fisiológicos, identidad genética, mental, económica, cultural o social de esa persona natural. Para evitar dudas, "Datos Personales" tiene el significado que se establece en el Reglamento y en las Leyes de Protección de Datos aplicables.

"Procesado" o "Tratamiento" significa cualquier operación o conjunto de operaciones que se realiza en Datos Personales o en conjuntos de Datos Personales, ya sea por medios automáticos o no, tales como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, revelación por transmisión, disseminación o puesta a disposición, alineación o combinación, restricción, borrado o destrucción.

"Reglamento" (RGPD) significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46 / EC.

"Violación de Datos Personales" significa una violación de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso, accidentales o ilegales, de Datos Personales transmitidos, almacenados o procesados de cualquier otra manera.

"Servicio" significa el Servicio que se acuerda prestar en el MSA;

"Categorías especiales de datos personales" significa Datos personales que revelan: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin exclusivo de identificar a una persona física, datos sobre la salud o los datos relativos a la vida sexual u orientación sexual de una persona física, incluidos los datos relacionados con condenas y delitos penales o medidas de seguridad relacionadas con lo anterior.

"Cláusulas contractuales estándar" o "Cláusulas Tipo" significa las cláusulas contractuales estándar para la transferencia de datos personales de un Responsable del Tratamiento de la UE a una entidad no perteneciente al EEE que actúa como Encargado del Tratamiento, adoptadas por la Comisión Europea en su Decisión 2010/87 / UE el 5 de febrero de 2010, incluyendo sus Apéndices 1 y 2 (los Anexos 1 y 2 a este DPA) adjuntos.

"Sub – encargado del tratamiento" significa una entidad contratada por el Encargado del Tratamiento para ayudarlo (o que lleva a cabo cualquier) Tratamiento de los Datos personales del Cliente en cumplimiento de las obligaciones del Encargado del Tratamiento de conformidad con el DPA, tal como figura en la Lista de sub - encargados, que ha sido aprobada por el Responsable del Tratamiento de datos de conformidad con la cláusula 5 de este DPA.

"Autoridad de Supervisión" significa cualquier autoridad que tenga la competencia de vigilar y hacer cumplir la aplicación de las Leyes de Protección de Datos aplicables relativas al Tratamiento de Datos Personales del Cliente, con respecto a la prestación del Servicio;

2. PAPELES EN LA PROTECCIÓN DE DATOS

2.1. Las Partes acuerdan lo que sigue:

- a) Este DPA se aplica únicamente cuando el Cliente actúa como Responsable del Tratamiento en relación con los Datos Personales del Cliente tratados por NOMINALIA durante la prestación del Servicio;
- b) NOMINALIA actúa como Encargado del Tratamiento de los Datos personales del Cliente, para la prestación del Servicio; y
- c) Este DPA regula la relación entre las Partes en cuanto a los respectivos deberes y obligaciones relacionados con el Tratamiento de los Datos personales del Cliente por parte del Encargado del Tratamiento, en la prestación del Servicio.

3. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

3.1. El Responsable del Tratamiento define el propósito del Tratamiento de los Datos Personales del Cliente para la prestación del Servicio.

3.2. Respecto a la prestación del Servicio, el Encargado del Tratamiento se compromete a asumir las siguientes obligaciones incluyendo las relacionadas en los anexos 1 y 2 al presente:

a) El Encargado del Tratamiento trata los Datos Personales del Cliente solo según sea necesario para proporcionar el Servicio, sujeto a las instrucciones escritas del Responsable del Tratamiento en el presente DPA;

b) El Encargado del Tratamiento notifica al Responsable del Tratamiento en caso de que considere que las instrucciones escritas del Responsable del Tratamiento infringen las Leyes de Protección de Datos aplicables. En ningún caso está el Encargado del Tratamiento obligado a realizar un examen legal detallado respecto de ninguna instrucción escrita del Cliente;

c) NOMINALIA como Encargado del Tratamiento notificará al Responsable del Tratamiento sin demora indebida de cualquier contacto o comunicación que reciba de una Autoridad de Supervisión en relación con el Tratamiento de los Datos Personales del Cliente. En este sentido, las Partes reconocen y acuerdan que la responsabilidad de responder a tales solicitudes recae en el Responsable del Tratamiento y no en el Encargado del Tratamiento.

d) El Encargado del Tratamiento ha implementado medidas operativas, técnicas y organizativas adecuadas, incluidas las descritas en el Anexo 2, para proteger los Datos Personales del Cliente. Las Partes reconocen y acuerdan que el Encargado del Tratamiento está específicamente autorizado para implementar medidas alternativas adecuadas o utilizar ubicaciones alternativas siempre que el nivel de seguridad de las medidas se mantenga o se refuerce en comparación con las medidas declaradas.

e) En caso de que el Encargado del Tratamiento revele Datos Personales del Cliente a su personal involucrado directa y exclusivamente en la ejecución del Servicio, el Encargado del Tratamiento se asegura de que dicho personal: i) tiene suscrito un compromiso de confidencialidad o tiene una obligación legal de confidencialidad y; ii) Procesa Datos Personales del Cliente bajo las instrucciones del Encargado del Tratamiento en cumplimiento de sus obligaciones bajo este DPA.

4. OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

4.1. El Responsable del Tratamiento reconoce y acepta que para que el encargado del Tratamiento preste el servicio, el Responsable del Tratamiento debe proporcionar al encargado del Tratamiento los datos personales del Cliente.

4.2. El Responsable del Tratamiento declara y garantiza que

- a) tiene una base legal apropiada (por ejemplo, consentimiento del Sujeto Titular de los Datos, intereses legítimos, autorización de la Autoridad de Supervisión pertinente, etc.) para tratar y comunicar Datos Personales al Encargado del Tratamiento como parte de la prestación del Servicio; y
- b) las estipulaciones de este DPA reflejan las obligaciones que las leyes aplicables imponen a NOMINALIA, relativas al tratamiento de los Datos Personales del Cliente para la prestación del Servicio.

5. AUTORIZACIÓN PARA EL SUB - TRATAMIENTO

5.1. El Responsable del Tratamiento reconoce, acepta y consiente que, con el único y exclusivo propósito de prestar el Servicio y sujeto siempre al cumplimiento de los términos de esta DPA, los Datos Personales del Cliente pueden ser Procesados por el Encargado del Tratamiento o sus Sub - encargados como se describe en la Lista de Sub - encargados.

5.2. De conformidad con la Cláusula 5.1., El Encargado del Tratamiento tiene una autorización general para contratar Sub – encargados siempre que el Encargado del Tratamiento:

- a) proporcione al Responsable del Tratamiento información previa sobre la identidad de los Sub - encargados como se describe en la Lista de Sub - encargados y notifique al Responsable del Tratamiento de cualquier actualización en la Lista de Sub - encargados para que el Responsable del Tratamiento pueda oponerse a la contratación de tales sub - encargados;
- b) celebre acuerdos con los Sub - encargados que contengan las mismas obligaciones relacionadas con el Tratamiento de los Datos Personales del Cliente como se establece en este DPA;

c) ejerza la debida diligencia al seleccionar a los Sub - encargados y siga siendo responsable del cumplimiento de los Sub - encargados con las obligaciones establecidas en este DPA;

d) a solicitud del Responsable del Tratamiento, el Encargado del Tratamiento proporciona al Responsable del Tratamiento información razonable sobre las acciones y medidas que el Encargado del Tratamiento y sus Sub - encargados han llevado a cabo para cumplir con las disposiciones establecidas en este Acuerdo de Protección de datos.

6. TRANSFERENCIA DE DATOS PERSONALES E INCLUSIÓN DE CLÁUSULAS – TIPO (SI FUESE APLICABLE)

6.1. En la medida en que el Reglamento sea aplicable y no existan Decisiones de Adecuación, el Responsable del Tratamiento y el Encargado del Tratamiento se comprometen a firmar las Cláusulas Contractuales Estándar. Además, el Responsable del Tratamiento autoriza expresamente la firma de las Cláusulas Contractuales Estándar, lo que permite al Encargado del Tratamiento suscribir las mismas con entidades no pertenecientes al EEE en nombre del Responsable del Tratamiento.

6.2. De conformidad con la Cláusula 6.1, las Partes reconocen que se aplicarán los Anexos 1 y 2 de esta DPA, y que los Anexos 1 y 2 se considerarán Apéndices 1 y 2 de las Cláusulas Contractuales Estándar. El Encargado del Tratamiento está autorizado por el Responsable del Tratamiento para modificar unilateralmente los Apéndices 1 y 2 de las Cláusulas Contractuales Estándar solo en la medida en que imponga obligaciones más estrictas a la Entidad que no es del EEE.

6.3. Nada en el DPA se interpretará como que prevalece sobre ninguna cláusula contradictoria de las Cláusulas Contractuales Estándar.

6.4. Previa solicitud, el Responsable del Tratamiento puede revisar las Cláusulas Contractuales Estándar, incluidos los Anexos 1 y 2.

6.5. El Responsable del Tratamiento reconoce que es su responsabilidad cumplir con cualquier obligación o deber adicionales con el fin de transferir los Datos Personales al Encargado o a los Sub-Encargados de conformidad con las leyes de Protección de Datos aplicables.

7. COOPERACIÓN Y OBLIGACIONES DE REGISTRO

7.1. Las Partes colaboran de buena fe para garantizar el cumplimiento de las disposiciones del presente DPA, incluido, pero no sólo, garantizar el ejercicio correcto y oportuno de los derechos del Titular, gestionando incidentes en caso de seguridad / violación de datos personales para mitigar su posibles efectos adversos.

7.2 Las Partes colaboran de buena fe para poner a disposición entre sí y a las Autoridades de Supervisión la información necesaria para demostrar el cumplimiento de las Leyes de Protección de Datos aplicables.

8. DERECHOS DEL TITULAR DE LOS DATOS (INTERESADO)

8.1. Teniendo en cuenta la naturaleza del Tratamiento, el Encargado del Tratamiento ayuda al Responsable del Tratamiento mediante medidas técnicas y organizativas apropiadas para el cumplimiento de la obligación del Responsable del Tratamiento de responder a las solicitudes de ejercicio de los derechos del Interesado.

8.2. El Encargado del Tratamiento proporcionará al Responsable del Tratamiento una cooperación y asistencia razonables y proporcionará la información que sea razonablemente necesaria para responder a los Interesados o alternativamente para permitir que el Responsable del Tratamiento cumpla con sus deberes conforme a las Leyes de Protección de Datos aplicables en relación con los derechos del Interesado. El responsable del Tratamiento reconoce y acepta que en caso de que tal colaboración y asistencia requieran el empleo de recursos significativos por parte del Encargado, esta colaboración será facturable mediando aviso a, y acuerdo con, el Responsable del Tratamiento.

9. DEVOLUCIÓN Y BORRADO DE DATOS

9.1. El Encargado del Tratamiento, sin coste alguno para el Responsable del Tratamiento, devolverá o destruirá los Datos Personales del Cliente a petición del Responsable del Tratamiento y al vencimiento o a la terminación anticipada de este DPA, previa solicitud escrita del Responsable del Tratamiento dada con un preaviso razonable, salvo que haya un mandato expreso legal (incluidas, entre otras, las Leyes de Protección de Datos aplicables o la autoridad encargada de hacer cumplir la ley), incluida, entre otras y pero no sólo, la Autoridad de Supervisión, que impida al Encargado hacer tal cosa.

9.2. Con respecto a las solicitudes específicas del Responsable del Tratamiento para la devolución de los Datos Personales del Cliente, dicha solicitud se cumplirá en la medida de lo posible, con sujeción a los condicionantes técnicos y organizativos razonables, que estarán en consonancia con el volumen, categoría y cantidad de los Datos Personales tratados.

9.3 Los Datos Personales devueltos siguiendo el procedimiento estándar de NOMINALIA lo serán sin coste para el Cliente; en otros supuestos se devolverán cargando un coste razonable al Cliente.

9.4. En caso de que el Responsable del Tratamiento opte por la eliminación de Datos Personales del Cliente y salvo lo dicho en la Cláusula 9.5, el Encargado del Tratamiento emitirá una declaración formal relativa a dicha eliminación.

9.5. El Encargado del Tratamiento puede retener Datos Personales del Cliente que se almacenan de acuerdo con operaciones regulares de respaldo informático de acuerdo con los protocolos de recuperación de

desastres y continuidad del negocio del Encargado del Tratamiento (ver Cláusula 12), siempre que el Encargado del Tratamiento no trate, y no permita sus Sub – encargados tratar, de manera activa o intencional, dichos Datos Personales del Cliente para cualquier fin que no sea la prestación del Servicio.

10. TRANSMISIONES

10.1. Los datos personales transmitidos por el Encargado del Tratamiento a través de Internet en relación con el Servicio, deberán estar razonablemente encriptados. Las Partes reconocen, sin embargo, que no se puede garantizar la seguridad de las transmisiones por Internet. El Encargado del Tratamiento no será responsable del acceso del responsable del Tratamiento a Internet, de ninguna interceptación o interrupción de cualquier comunicación vía internet, ni por cambios y pérdidas de Datos Personales vía Internet.

10.2. Si se sospecha de alguna Violación de Datos Personales, el Encargado del Tratamiento puede suspender el uso del Servicio por parte del Responsable del Tratamiento a través de Internet, en espera de una investigación, siempre que el Encargado del Tratamiento notifique dicha suspensión tan pronto como sea razonablemente posible y tome todas las medidas razonables para restablecer rápidamente el uso del Servicio a través de Internet y cooperar con el Responsable del Tratamiento para continuar la prestación del Servicio a través de otros canales de comunicación.

10.3 El Responsable del Tratamiento tomará y emprenderá todas las medidas y acciones necesarias para mantener la confidencialidad de los nombres y contraseñas de los empleados del Responsable del Tratamiento para los Servicios. El Responsable del Tratamiento lo será de las consecuencias de cualquier mal uso del Servicio por parte de cualquiera de sus empleados.

11. VIOLACIÓN DE DATOS PERSONALES

11.1 El Responsable del Tratamiento reconoce y acepta que el Encargado del Tratamiento no se considerará responsable por la violación de Datos Personales no imputable a la negligencia del Encargado del Tratamiento.

11.2 Si el Encargado del Tratamiento se entera de una Violación de Datos Personales, deberá:

- a) tomar las medidas apropiadas para contener y mitigar dicha Violación de Datos Personales, incluida la notificación al Responsable del Tratamiento lo antes posible, para permitir que el Responsable del Tratamiento implemente rápidamente su programa de respuesta. Sin perjuicio de lo anterior, el Encargado del Tratamiento se reserva el derecho a determinar las medidas a adoptar para cumplir con las leyes de Protección de Datos aplicables o para proteger sus derechos e intereses;
- b) cooperar con el Responsable del Tratamiento para investigar: la naturaleza, las categorías y el número aproximado de Interesados afectados, las categorías y el número aproximado de registros de Datos Personales afectados y las consecuencias probables de cualquier Violación

de Datos Personales de una manera acorde con su importancia y su impacto general en el Responsable del Tratamiento y la prestación del Servicio según este DPA;

- c) cuando las Leyes de Protección de Datos aplicables requieran la notificación a las Autoridades Supervisoras pertinentes y a los Interesados afectados por dicha Violación de Datos Personales, y en la medida en que tenga relación con los Datos Personales del Cliente, comunicar a y recibir instrucciones del Responsable del Tratamiento, que como Responsable del Tratamiento tiene el derecho exclusivo para determinar las medidas que haya que tomar para cumplir con las Leyes de Protección de Datos Aplicables o para remediar cualquier riesgo, incluyendo, pero no sólo:
 - i. si el aviso se debe dar a personas, organismos reguladores, agencias de aplicación de la ley, agencias de información al consumidor, u otros, según lo requieran las Leyes de Protección de Datos aplicables, o a la discreción del Responsable del Tratamiento; y
 - ii. el contenido de dicha notificación, ya sea que se ofrezca algún tipo de solución a los Interesados afectados, y la naturaleza y el alcance de dicha solución.

12. RECUPERACION DE DESASTRES Y CONTINUIDAD DEL NEGOCIO

12.1 El Encargado del Tratamiento mantiene protocolos de continuidad de negocio y recuperación de desastres comercialmente razonables, cuya copia resumida está disponible para su visualización por el Responsable del Tratamiento, a solicitud de éste. El Encargado del Tratamiento puede modificar dicho plan en cualquier momento, siempre que no reduzca su capacidad de recuperación de desastres por debajo de la capacidad de recuperación de desastres vigente de acuerdo con el plan que exista a la fecha.

13. MANDATO

13.1 Con la firma del presente DPA, incluidos Anexos 1, 2 y 3, el Responsable del Tratamiento ordena explícitamente al Encargado del Tratamiento I que lleve a cabo en nombre del Responsable del Tratamiento las actividades descritas en las Cláusulas 5 y 6 anteriores.

13.2 Con la firma del presente DPA, el Encargado del Tratamiento acepta el mandato, que se llevará a cabo sin remuneración económica, ya que está en conexión con el Servicio, y legalmente significa que el Encargado del Tratamiento ha leído y entendido las instrucciones asignadas.

ANEXO 1 (Apéndice 1 de las Cláusulas contractuales estándar, cuando corresponda)

1. EXPORTADOR DE DATOS

El exportador de datos / Responsable del Tratamiento es: el Responsable del Tratamiento definido en la cláusula 1 del DPA o el Encargado del Tratamiento autorizado por aquél de conformidad con la cláusula 6 del DPA.

2. IMPORTADOR DE DATOS

El importador de datos / Encargado del Tratamiento es el Encargado del Tratamiento como se define en la Cláusula 1 del DPA o el Sub-encargado, según lo autorizado por el Responsable del Tratamiento en las Cláusulas 5 y 6 del DPA.

3. INTERESADOS

Los datos personales transferidos / tratados, de acuerdo con el Servicio específico contratado, pueden afectar a las siguientes categorías de datos personales:

- Cliente y/o empleados y colaboradores del Cliente;
- Proveedores del Cliente;
- Usuarios del Cliente;
- Clientes del Cliente,
- Titulares de Datos cuyos Datos personales se procesan por el Cliente actuando éste como Responsable del Tratamiento usando los Servicios prestados por NOMINALIA;

4. CATEGORÍAS DE DATOS PERSONALES

Los datos personales transferidos / tratados para prestar cualquier servicio al Cliente, que no se puedan determinar por anticipado, se refieren exclusivamente a los Datos personales conforme al significado indicado en el artículo 4 (1) del Reglamento, quedando expresamente excluidos los Datos Personales relativos a antecedentes penales y a categorías especiales de datos:

- Datos de contacto (nombre, apellidos, dirección de correo electrónico, dirección postal, número de teléfono);
- Fecha de nacimiento;
- Edad;
- Género;

- Otras categorías de datos personales tratados por el Cliente actuando como Responsable del Tratamiento usando los servicios PRestados por NOMINALIA;

5. CATEGORÍAS ESPECIALES DE DATOS

Los datos personales comunicados / tratados no son datos relativos a antecedentes penales ni categorías especiales de datos.

6. OPERACIONES DE TRATAMIENTO

Los datos personales serán tratados / comunicados solamente para prestar el Servicio descrito en el MSA.

ANEXO 2 (Apéndice 2 a las Cláusulas Contractuales Estándar, cuando sea aplicable)

Descripción de las Medidas Organizativas y de Seguridad

El Encargado del Tratamiento y los Sub –Encargados se comprometen a mantener al menos las medidas técnicas y orgnizativas descritas a continuación.

Procedimientos de Seguridad de la Información

Organización Interna

Se han definido funciones y responsabilidades para la seguridad de la información y se han asignado a las personas de la Empresa a cargo de las actividades de Tratamiento (en adelante, “usuarios”) con el fin de evitar conflictos de interés y de prevenir actividades inapropiadas.

Seguridad en materia de Recursos Humanos

Dispositivos móviles y teletrabajo

Hay una Política de Seguridad para el uso de todos los dispositivos de la Empresa, en particular dispositivos móviles, y se han implantado controles adecuados.

Terminación o cambios en la relación contractual de trabajo

A la terminación del contrato de trabajo de un usuario o en caso de un cambio significativo en su posición dentro de la Empresa, se actualizan de forma inmediata los permisos de acceso, a la vez que las herramientas de trabajo se devuelven y resetean tanto físicamente como en su contenido y programación.

Gestión de los activos de la Empresa

Responsabilidad de los recursos y activos de la Empresa

Todas las herramientas y activos se han inventariado cuidadosamente y se vigila la asignación de cada uno de ellos a los diversos usuarios responsables. Se ha definido además una Política para su uso correcto.

Clasificación de la información

Toda la información se clasifica y cataloga por los respectivos usuarios en línea con los requisitos de seguridad, así como se procesa adecuadamente.

Gestión de Medios

Toda la información almacenada en los diferentes soportes se clasifica , controla, modifica y usa de modo que su contenido no se ve comprometido; y se borra de una forma adecuada.

Control de accesos

Requisitos empresariales para el control de acceso

Los requisitos organizativos de la Empresa para monitorear el acceso a los recursos de información están documentados en una Política y puestos en práctica mediante procedimientos de acceso. Los accesos a la Red y conexiones están restringidos.

Gestión de acceso de usuario

La asignación de los derechos de acceso de los usuarios se controla desde el registro inicial del usuario hasta la eliminación de los derechos de acceso cuando ya no son necesarios, incluidas las restricciones especiales sobre derechos de acceso privilegiado y la gestión de "información secreta de autenticación", y está sujeta a comprobaciones y revisiones periódicas, incluida la actualización de los derechos de acceso cuando sea necesario. En la gestión de los accesos, se aplica el criterio de minimizar los derechos de acceso, ya que éstos se emiten para dar al usuario solamente el acceso a los datos que sea necesario para su trabajo y funciones en el negocio. Los derechos de acceso adicionales requieren autorizaciones específicas.

Responsabilidad del usuario

Los usuarios son conscientes de sus responsabilidades mediante un control de acceso efectivo, por ejemplo, eligiendo una contraseña compleja cuya complejidad se verifica por el sistema, y manteniéndola confidencial.

Sistemas y aplicaciones para control de acceso

El acceso a la información está sujeto a restricciones de conformidad con la política de control de accesos, mediante un sistema de acceso seguro y administración de contraseñas de acceso, así como mediante el control de utilidades privilegiadas y acceso limitado a todos los códigos fuente.

Cifrado o encriptación

Control criptográfico

Existe una Política sobre encriptación de medios y datos de usuarios. Las claves / autenticaciones están encriptadas.

Seguridad física y del entorno

Hay implementadas medidas de seguridad físicas y de entorno con el fin de prevenir accesos accidentales o ilegítimos, así como la pérdida o la revelación de datos.

Áreas seguras: centro de datos.

Los servicios de la Empresa se prestan desde y alojan en varios centros de datos en diversas partes del mundo, uno de los cuales que guarda datos personales de clientes es uno de los pocos certificados como Tier IV en Italia, que es la máxima garantía que un centro puede ofrecer. Todos los centros de datos en la cadena de Servicio disponen de sistemas eléctricos, de refrigeración y de red redundantes. Todos los centros de datos tienen sistemas de iluminación perimetral y detectores de presencia con cámaras de seguridad. Las puertas de emergencia están equipadas con alarmas. Todas las alarmas están concentradas en cuartos de control.

El acceso físico se regula y controla con procedimientos de autorización, reconocimiento y registro, y se limita, gracias al control de accesos, a las áreas para las que se ha dado la autorización.

Equipo

Hay una Política implementada para deshacerse del equipo sobrante, con el fin de destruir de modo seguro toda la información contenida en el mismo.

Seguridad de las Operaciones

Procedimientos y responsabilidades operacionales

Las responsabilidades operativas en IT están documentadas, y se controlan los cambios en las instalaciones y sistemas de IT. Los sistemas de desarrollo, prueba y operativos están separados. Hay usuarios responsables del correcto funcionamiento de los procedimientos. Por otra parte, la gestión de la seguridad lógica de los sistemas operativos y de las aplicaciones instaladas por el Cliente es la responsabilidad del cliente de los servicios individuales facilitados por la Empresa (en adelante, también “el Cliente”).

Protección contra malware

Hay controles activos de virus y malware en los dispositivos de la Compañía, y los usuarios están adecuadamente informados y advertidos.

En cuanto a los servicios de Servidor Virtual y Servidor Dedicado, el cliente es responsable de instalar antivirus y software anti-malware y, si el correspondiente servicio no se ha adquirido, de instalar un firewall.

En cuanto al servicio de alojamiento (hosting), existe una protección en tiempo real instalada en las máquinas.

En cuanto al servicio de correo electrónico, el tráfico de correo se analiza en tiempo real, tanto saliente como entrante, para detectar virus, malware y para la identificación y filtrado de spam. El análisis es automático y se basa en la naturaleza del contenido, en la consulta a bases de datos internacionales, y en la reputación adquirida con base en una serie de parámetros.

Backup

Se hacen y preservan copias de seguridad con la exclusión de servicios para los que el Cliente es responsable de mantener y de gestionar sus propias copias de seguridad (Servidores Dedicados y Virtuales). Para los servicios de alojamiento y correo, se hacen backups periódicamente, que en el caso del Hosting también pueden ser accedidos por el Cliente. Backups adicionales a los que no tiene acceso el Cliente se hacen regularmente solo con la finalidad de Recuperación de Desastres.

Autenticación y monitorización

Autenticación y sincronización

Todas las actividades y eventos relacionados con la seguridad de la información suceden tras la introducción por parte de los usuarios / administradores de sus claves de autenticación o certificados de identidad. Los relojes de todos los equipos están sincronizados.

Control del software operativo

La instalación del software en los sistemas operativos debe estar controlada y monitorizada.

En cuanto a los Servidores Virtuales y Dedicados, los sistemas operativos que se facilitan a los clientes se ponen a disposición de éstos con imágenes de instalación as, incluso durante la instalación por el propio cliente. Es también responsabilidad del cliente actualizar el software de firma y las aplicaciones o software por él instalados.

Gestión de vulnerabilidades / debilidades técnicas

Gestión de parches

Cada vulnerabilidad técnica se corrige con parches adecuados; y hay procedimientos para todas las fases de prueba y para la instalación subsiguiente del software y de sus actualizaciones, lo que tiene lugar solamente cuando todas las pruebas son positivas.

Consideraciones de auditoría de sistemas de información

Se hacen auditorías periódicas de IT con el fin de minimizar cualquier efecto negativo en los sistemas de producción y para asegurar que no hay ningún acceso no autorizado a datos.

Seguridad de las comunicaciones

Gestión de seguridad de red

Las redes y los servicios en línea tdeben protegerse, por ejemplo por medio de su separación y segregación.

Transferencia de información

Hay acuerdos vigentes relativos a la transferencia de información de y hacia terceros.

Adquisición, desarrollo y mantenimiento del Sistema

Seguridad en procesos de desarrollo y soporte

Las reglas que rigen la seguridad del software y el desarrollo del sistema están definidas en una Política. Los cambios en el sistema (tanto para aplicaciones como para sistemas operativos) se controlan siempre. La seguridad de los sistemas se comprueba y se han definido criterios de idoneidad que incluyen aspectos de seguridad.

Relación con los proveedores

Seguridad de la información en la relación con los proveedores

Hay contratos o acuerdos destinados a proteger el tratamiento de la información de la organización y de clientes que esté accesible a terceros proveedores de IT, así como a otros terceros que forman parte de la cadena de suministro.

Gestión de servicios prestados por el proveedor

La prestación de servicios prestados por proveedores externos se supervisa y verifica / audita en relación con el/los contratos o acuerdos. Se comprueban todos los cambios en el servicio.

Gestión de incidentes en materia de seguridad de la información

Gestión de incidentes de seguridad de la información y mejoras

Hay responsabilidades y procedimientos específicos destinados a gestionar (reportar, asegurar, responder y aprender de) de forma coherente y eficaz los eventos e incidentes relacionados con la seguridad de la información (por ejemplo, el denominado procedimiento de *Violación de Datos*).

Aspectos de seguridad de la información relacionados con la continuidad del negocio

Redundancias

Todas las instalaciones importantes de IT tienen sistemas redundantes de forma suficiente para garantizar los requisitos de disponibilidad.. Cuando no hay tal redundancia instalada, se han implementado las medidas adecuadas para asegurar la continuidad del servicio o la minimización de la pérdida de datos.

Compliance

Cumplimiento de requisitos legales y contractuales

La compañía identifica y documenta sus obligaciones frente a autoridades externas y otros terceros en relación con la seguridad de la información, incluida la propiedad intelectual, documentación contable, e información sobre privacidad.

Revisión de la seguridad de la información

Se revisan de forma periódica los proyectos de la Organización relativos a la seguridad de la información y a las políticas de seguridad, y se aplican medidas correctoras cuando es necesario.

ANEXO 3 (Lista de Sub-encargados)

Se puede obtener la lista de sub – encargados enviando un email a dpo@nominalia.com

ACUERDO DE TRATAMIENTO DE DATOS PARA CLIENTES QUE SOLICITAN LOS SERVICIOS DE NOMINALIA EN NOMBRE DE TERCEROS

II. PREÁMBULO

Considerando:

A. El Cliente, en relación con los servicios prestados a sus clientes, normalmente actúa como Encargado del Tratamiento –; por su parte los Clientes, según corresponda, pueden actuar como Responsables del Tratamiento o como Encargados del Tratamiento ellos mismos (“Cliente” o “Clientes”);

B. En el contexto de la prestación de esos servicios, el Cliente puede contratar sub – encargados para prestar tales servicios en su nombre. Donde el Cliente actúa como Encargado del Tratamiento, esos subcontratistas se considerarán igualmente Encargados del Tratamiento, conforme al Reglamento UE 2016/679 (en adelante, **RGPD**).

C. El Cliente desea regular sus relaciones de tratamiento de datos con los sub – encargados, por medio de un acuerdo escrito conforme con los requisitos del artículo 28 del RGPD.

D. Este Acuerdo de Sub - Tratamiento de Datos, junto con sus Anexos (en conjunto "**DSPA**") se celebra entre el Cliente (en adelante, **Cliente** o **Encargado del Tratamiento**) y la entidad o persona física que solicita el Servicio, como se define más abajo – en nombre de terceros con el fin de revender tal servicio o no, y **NOMINALIA** (en adelante, el **Sub – Encargado** del Tratamiento o **NOMINALIA**); el Cliente y **NOMINALIA** en conjunto, las "**Partes**" y singularmente cada uno de ellos como la "**Parte**", suscriben con el fin de reflejar el acuerdo de las Partes con respecto al Tratamiento de Datos Personales en relación con el Servicio ("**Datos Personales del Cliente**"), de conformidad con los requisitos de las Leyes de Protección de Datos aplicables.

E. **NOMINALIA** ha acordado prestar el servicio o los servicios al Cliente (el **Servicio**) en los términos del acuerdo alcanzado con la Orden de Servicio y las Condiciones Generales de Servicio disponibles en el enlace <https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/> (en adelante, el **Acuerdo Master**).

F. El objeto, naturaleza y propósito del Tratamiento de Datos Personales del Cliente relacionado con el Servicio, así como el tipo de Datos Personales y las categorías de Interesados, se describen con mayor detalle en el Anexo 1 al presente **DSPA**.

G. Las partes han suscrito este **DSPA** con el fin de asegurarse de que cumplen con las Leyes de Protección de Datos aplicables, y para establecer salvaguardas y procedimientos para el tratamiento conforme a la normativa de Datos Personales.

Este Preámbulo forma parte integral de este Documento.

1. DEFINICIONES

Salvo que se diga otra cosa en este **DSPA**, todos los términos con mayúsculas aquí empleados tendrán el significado que se les da en el Acuerdo. En caso de conflicto o de incongruencia en términos de las salvaguardias de protección de datos entre el **DSPA** y el Acuerdo, este **DSPA** prevalecerá.

“**Leyes Aplicables de Protección de Datos**” significa, en los países miembros de la UE, el Reglamento y las leyes complementarias en materia de Protección de Datos en esos países, incluyendo cualquier guía y/o códigos de prácticas emitidos por la Autoridad de Supervisión correspondiente en la UE; en países no miembros de la UE, cualquier ley de protección de los Datos Personales relativa a la salvaguardia y tratamiento conforme a ley de Datos Personales.

“**Datos Personales del Cliente**” significa Datos Personales relativos a Titulares de Datos (“Interesados”), tratados en relación con el Servicio,

“**Responsable del Tratamiento**” en general significa la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determina el objeto y significado del tratamiento de datos personales.

“**Encargado del Tratamiento**” significa en general la persona física o jurídica, autoridad pública, agencia u otro organismo que trata datos en nombre del Responsable.

“**Titular de los Datos**” o “**Interesado**” tiene el significado que se le da en el RGPD.

“**Derechos del Interesado**” significa los derechos que se le reconocen al Interesado de conformidad con las leyes de Protección de Datos aplicables. En la medida en que el Reglamento (RGPD) es aplicable, “Derechos del Interesado” significa, por ejemplo, el derecho a pedir al Responsable del Tratamiento acceso, rectificación o supresión de los Datos o limitaciones al tratamiento relativas al Interesado o negarse al tratamiento así como pedir la portabilidad.

“**DSPA**” significa este Acuerdo Global de Sub - Tratamiento de Datos junto con sus Anexos.

“**GDPR**” (o “Reglamento”) significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46 / EC.

“**Lista de Sub – Encargados**” indica la que está disponible enviando una solicitud al respecto a dpo@nominalia.com

“**Acuerdo Master**” indica los términos y condiciones contenidos en la Orden u Órdenes de Servicio y en los Términos y Condiciones de Servicio relativos a la prestación del mismo acordadas entre las Partes y

disponibles en el siguiente enlace <https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/>

“Datos Personales” significa cualquier información relacionada con una persona física identificada o identificable; una persona física identificable es aquella que puede identificarse, directa o indirectamente, en particular por referencia a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos de los factores físicos, fisiológicos, identidad genética, mental, económica, cultural o social de esa persona natural. Para evitar dudas, **“Datos Personales”** tiene el significado que se establece en el RGPD y en las Leyes de Protección de Datos aplicables.

“Violación de Datos Personales” significa una violación de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso, accidentales o ilegales, de Datos Personales transmitidos, almacenados o procesados de cualquier otra manera.

“Procesado” o **“Tratamiento”** significa cualquier operación o conjunto de operaciones que se realiza en Datos Personales o en conjuntos de Datos Personales, ya sea por medios automáticos o no, tales como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, revelación por transmisión, diseminación o puesta a disposición, alineación o combinación, restricción, borrado o destrucción.

“Encargado del Tratamiento” significa en general la persona física o jurídica, autoridad pública, agencia u otro organismo que trata datos en nombre del Responsable. Para los fines de este DPA, el Encargado del Tratamiento es NOMINALIA.

“Categorías especiales de datos personales” significa Datos personales que revelan: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin exclusivo de identificar a una persona física, datos sobre la salud o los datos relativos a la vida sexual u orientación sexual de una persona física, incluidos los datos relacionados con condenas y delitos penales o medidas de seguridad relacionadas con lo anterior.

“Servicio” es el servicio descrito en el Acuerdo Master;

“Sub – Encargado” es la entidad identificada por el Encargado del Tratamiento para asistirle (o para asumir directamente) en el tratamiento de datos personales del Cliente en cumplimiento de las obligaciones establecidas por el Encargado del Tratamiento y que se mencionan en este DSPA;

“Autoridad de Supervisión” significa cualquier autoridad que tenga la competencia de vigilar y hacer cumplir la aplicación de las Leyes de Protección de Datos aplicables relativas al Tratamiento de Datos Personales del Cliente, con respecto a la prestación del Servicio;

2. PAPELES EN LA PROTECCIÓN DE DATOS

Las Partes acuerdan lo que sigue:

- d) Este DSPA se aplica exclusivamente en los casos en que el Cliente y NOMINLAIA son los dos Encargados del Tratamiento en relación con los Datos Personales del Cliente tratados en el contexto de la prestación del Servicio;
- e) Los Clientes a los que se les preste el Servicio actuarán como Responsables del Tratamiento, o como Encargados del Tratamiento en representación de aquéllos (por ejemplo, los usuarios finales de esos Clientes);
- f) NOMINLAIA ha sido contratada por el Cliente para prestar el Servicio, en su representación, a los clientes de ésta; y
- g) Este DSPA regula la relación entre las Partes en cuanto a los respectivos deberes y obligaciones relacionados con el Tratamiento de los Datos personales del Cliente por parte del Sub - Encargado, en el contexto de la prestación del Servicio.

3. OBLIGACIONES DEL SUB - ENCARGADO DEL TRATAMIENTO

3.1. El Sub - Encargado del Tratamiento se compromete a asumir las siguientes obligaciones, incluyendo las contenidas en los Anexos 1, 2 y 3, que se consideran partes integrantes de este DSPA:

- a) El Sub - Encargado del Tratamiento tratará los Datos Personales del Cliente solo según sea necesario para proporcionar el Servicio, y sujeto a las instrucciones escritas del Cliente, incluyendo lo estipulado en el Acuerdo y en el presente DSPA;
- b) El Sub - Encargado del Tratamiento informará al Cliente en caso de que considere que las instrucciones escritas recibidas de ésta infringen las Leyes de Protección de Datos aplicables;
- c) El Sub - Encargado del Tratamiento notificará al Cliente, sin demora indebida, sobre cualquier contacto o comunicación que reciba de una Autoridad de Supervisión en relación con el Tratamiento de los Datos Personales del Cliente;
- d) El Sub - Encargado del Tratamiento ha implementado medidas operativas, técnicas y organizativas adecuadas, conforme al artículo 32 RGPD, para proteger los Datos Personales del Cliente. Las Partes conocen y acuerdan y están conformes con que el Sub - Encargado está además autorizado para implementar además otras medidas operativas, técnicas y organizativas o para establecer lugares alternativos de almacenamiento de datos teniendo en cuenta que el nivel de seguridad de las medidas o lugares escogidos, es, siempre, adecuado;

e) En caso de que el Sub - Encargado del Tratamiento revele Datos Personales del Cliente a su personal involucrado directa y exclusivamente en la ejecución del Servicio, el Sub - Encargado del Tratamiento se asegurará de que dicho personal:

i) tiene suscrito un compromiso de confidencialidad o tiene una obligación legal de confidencialidad y;

ii) Procesa Datos Personales del Cliente bajo las instrucciones del Sub - Encargado del Tratamiento, y en cumplimiento de las obligaciones de éste bajo este DSPA.

4. COOPERACIÓN Y OBLIGACIONES DE REGISTRO

4.1. Las Partes colaboran de buena fe para garantizar el cumplimiento de las disposiciones del presente DSPA y asistir a los Responsables del Tratamiento en el cumplimiento de sus obligaciones conforme a las Leyes de Protección de Datos aplicables, incluido, entre otros pero no sólo, garantizar el ejercicio correcto y oportuno de los derechos del Interesado, gestionando incidentes en caso de seguridad / violación de datos personales para mitigar su posibles efectos adversos.

4.2 Las Partes colaborarán de buena fe para poner a disposición entre sí y ante las Autoridades de Supervisión la información necesaria para demostrar el cumplimiento de las Leyes de Protección de Datos aplicables.

4.3 El Sub – Encargado permitirá y colaborará en las auditorías, incluyendo inspecciones dirigidas por el Cliente, los Responsables del Tratamiento o auditores encargados para ello por el Cliente o por los Responsables del Tratamiento, en los sistemas y sedes del Sub – Encargado en los que éste procesa datos personales. Las auditorías e inspecciones se harán previo aviso con tiempo razonable al Sub – encargado y no interferirán en la actividad habitual de éste. Cualquier información recogida en relación con las actividades del Sub – Encaragado será tratada de forma estrictamente confidencial, salvo en los casos en los que las normas imperativas aplicables en materia de protección de datos (incluyendo, pero no solo, las Leyes en la materia) o las órdenes vinculantes de las autoridades competentes (incluyendo, pero no sólo, la Autoridad de Supervisión) requieran que esa información sea revelada.

5. AUTORIZACION PARA EL TRATAMIENTO DE DATOS POR OTROS SUB – ENCARGADOS

5.1 El Cliente reconoce, acepta y consiente que, con el solo propósito de prestar el Servicio y en consonancia con las cláusulas de este DSPA, los Datos Personales del Cliente pueden tratarse por sub – encargados adicionales, como se describe en la lista de sub – encargados.

5.2 En consecuencia con lo anterior, NOMINALIA está autorizada a emplear sub – encargados adicionales, siempre teniendo en cuenta que:

- a) Informa al Encargado de la identidad de los sub – encargados por anticipado, como se describe en la lista de sub – encargados y notifica al Encargado de cualquier actualización en la citada lista, de modo que el Encargado pueda oponerse si quiere a la inclusión de tales sub – encargados;
- b) Firma acuerdos con los sub – encargados que contienen las mismas obligaciones que se contienen en el presente DSPA relativas al tratamiento de los datos personales del Cliente;
- c) Ejercita controles adecuados en la selección de los sub – encargados y es responsable del cumplimiento por parte de los sub – encargados de las obligaciones contenidas en el presente DSPA;
- d) A solicitud del Encargado, el sub – encargado facilita a aquél la información adecuada relativa a las acciones y medidas adoptadas por el sub – encargado y sus sub – encargados adicionales para asegurar el cumplimiento de las estipulaciones de este DSPA.

6. DERECHOS DEL TITULAR DE LOS DATOS (INTERESADO)

6.1. Teniendo en cuenta la naturaleza del Tratamiento, el Sub - Encargado del Tratamiento ayudará, adoptando las medidas técnicas y organizativas apropiadas, al Cliente en el cumplimiento de la obligación de éste a colaborar con los Responsables del Tratamiento de responder a las solicitudes de ejercicio de derechos de los Interesados.

6.2. El Sub - Encargado del Tratamiento prestará al Cliente una cooperación y asistencia razonables y proporcionará la información que sea razonablemente necesaria para permitir que los Responsables del Tratamiento cumplan con sus deberes conforme a las Leyes de Protección de Datos aplicables en relación con los derechos del Interesado.

7. DEVOLUCIÓN Y BORRADO DE DATOS

7.1. Sin perjuicio de lo indicado en 7.5, el Sub - Encargado del Tratamiento, sin coste alguno para el Cliente y a petición de éste, devolverá a éste los Datos Personales del Cliente (borrando todas las copias de los datos del Cliente que pudiera haber en posesión del Sub – Encargado), o bien borrará los datos personales del Cliente, sin retraso indebido y en todo caso no más tarde de 15 días después de recibir la petición del Cliente.

7.2. Sin perjuicio de lo indicado en 7.5, a la terminación por transcurso normal o anticipada de este DSPA, el Sub – Encargado deberá, sin coste para el Cliente, devolver los datos Personales del Cliente al Encargado (borrando todas las copias de los Datos personales del Cliente que estén en posesión del Sub – Encargado) sin retraso indebido y en todo caso no más tarde de 30 (treinta) días después de la terminación de este DSPA, salvo que por parte del Cliente se haya requerido otra cosa.

7.3. Las cláusulas 7.1 y 7.2 no se aplican cuando leyes imperativas (incluyendo, pero no sólo, las relativas a Protección de Datos) u órdenes emitidas por autoridades competentes (incluyendo, pero no solo, las Autoridades de Supervisión en la materia), impidan al Sub – Encargado cumplir tales cláusulas. El Sub – Encargado debe notificar al Cliente en tales casos, facilitando adecuada justificación y razonamiento relativos a su obligación legal de retener los datos personales del Cliente, sin retraso indebido y no más tarde de 10 (diez) días después de recibir la solicitud del Cliente, o la expiración o terminación anticipada de este DSPA; lo que sea de aplicación. El Sub – Encargado continuará vinculado por las cláusulas de este DSPA (incluso después de su expiración o terminación anticipada) en relación con cualquier Dato Personal de Cliente conservado por él conforme a esta Cláusula, y no deberá tratar ni activa ni intencionadamente tales Datos por ningún otro propósito que no sea el de cumplir con las citadas obligaciones u órdenes.

7.4 En cualquiera de los casos en los que los Datos Personales del Cliente se devuelven al Cliente (con borrado de todas las copias en posesión del Sub – Encargado) o se borran a su requerimiento, conforme a los apartados 7.1 y 7.2, el Sub – Encargado emitirá una declaración formal relativa a dicha devolución / eliminación, sin retraso y no más tarde de treinta (30) días después de la fecha en que se hayan realizado las indicadas devolución o eliminación.

7.5. El Sub -Encargado del Tratamiento puede retener Datos Personales del Cliente que se almacenan de acuerdo con operaciones regulares de respaldo informático de acuerdo con los protocolos de recuperación de desastres y de continuidad del negocio del Sub - Encargado del Tratamiento, siempre que el Sub - Encargado del Tratamiento y cualquiera de sus sub – encargados no traten de manera activa ni intencional, dichos Datos Personales del Cliente para cualquier otro fin que no sea la prestación del Servicio. El Sub – Encargado continuará vinculado por las cláusulas de este DSPA (incluso después de su expiración o terminación anticipada) en relación con cualquier Dato Personal de Cliente conservado por él conforme a esta Cláusula.

8. VIOLACIÓN DE DATOS PERSONALES

8.1 Si el Encargado del Tratamiento se entera de una Violación de Datos Personales, deberá:

- a) tomar las medidas apropiadas para contener y mitigar dicha Violación de Datos Personales, incluida la notificación al Cliente lo antes posible a partir del momento en que el Sub - Encargado del Tratamiento tenga conocimiento de dicha Violación de Datos Personales;
- b) cooperar con el Cliente y/o los Responsables del Tratamiento para investigar la naturaleza, las categorías y el número aproximado de Interesados afectados, las categorías y el número aproximado de registros de Datos Personales afectados y las consecuencias probables de cualquier Violación de Datos Personales de una manera acorde con su importancia y su impacto general en el Responsable del Tratamiento y la prestación del Servicio según el Acuerdo Master;

c) cuando las Leyes de Protección de Datos aplicables requieran la notificación a las Autoridades Supervisoras pertinentes y a los Interesados afectados por dicha Violación de Datos Personales, contactar y recibir instrucciones del Cliente y/o de los Responsables del Tratamiento, en la medida en que los Datos Personales del Cliente se hayan visto involucrados en la Violación – los Responsables del Tratamiento tienen el derecho exclusivo para determinar las medidas que haya que tomar para cumplir con las Leyes de Protección de Datos Aplicables o para remediar cualquier riesgo, incluyendo, pero no sólo:

- i. si el aviso se debe dar a personas, organismos reguladores, agencias de aplicación de la ley, agencias de información al consumidor, u otros, según lo requieran las Leyes de Protección de Datos aplicables, o a la discreción del Responsable del Tratamiento; y
- ii. el contenido de dicha notificación, ya sea que se ofrezca algún tipo de solución a los Interesados afectados bajo la responsabilidad del Responsable del Tratamiento, y la naturaleza y el alcance de dicha solución.

9. RECUPERACION DE DESASTRES Y CONTINUIDAD DEL NEGOCIO

9.1 El Sub - Encargado del Tratamiento mantiene protocolos actualizados de continuidad de negocio y de recuperación de desastres que varían según el Servicio de que se trate, comercialmente razonables, cuya copia resumida está a disposición del Responsable del Tratamiento a su solicitud. El Sub - Encargado del Tratamiento puede modificar dicho plan en cualquier momento, siempre que no reduzca su capacidad de recuperación de desastres por debajo de la capacidad de recuperación de desastres vigente de acuerdo con el plan que existe a la fecha de firma del presente DSPA.

ANEXO 1

1. INTERESADOS

Los datos personales del Cliente que sean tratados, dependiendo del Servicio de que se trate, pueden pertenecer a las siguientes categorías de Interesados (no se puede determinar por anticipado):

- Cliente y/o empleados y colaboradores del Cliente;
- Proveedores del Cliente;
- Usuarios del Cliente;
- Clientes del Cliente,
- Titulares de Datos cuyos Datos personales se procesan por el Cliente actuando éste como Responsable del Tratamiento usando los Servicios prestados por NOMINALIA;

2. CATEGORÍAS DE DATOS PERSONALES

Los datos personales tratados para prestar cualquier servicio al Cliente, que no se puedan determinar por anticipado, se refieren exclusivamente a los Datos personales conforme al significado indicado en el artículo 4 (1) del Reglamento, quedando expresamente excluidos los Datos Personales relativos a antecedentes penales y a categorías especiales de datos:

- Datos de contacto (nombre, apellidos, dirección de correo electrónico, dirección postal, número de teléfono);
- Fecha de nacimiento;
- Edad;
- Género;
- Otras categorías de datos personales tratados por el Cliente actuando como Responsable del Tratamiento usando los servicios PRestados por NOMINALIA;

3. CATEGORÍAS ESPECIALES DE DATOS (si fuese aplicable)

Los datos personales comunicados / tratados no son datos relativos a antecedentes penales ni categorías especiales de datos.

4. OPERACIONES DE TRATAMIENTO

Los datos personales serán tratados / comunicados solamente para prestar el Servicio descrito en el MSA.

ANEXO 2

Descripción de las Medidas Organizativas y de Seguridad

El Sub - Encargado se compromete a mantener al menos las medidas técnicas y orgnizativas descritas a continuación.

Información sobre las Medidas de Seguridad

La organización define los roles y responsabilidades para la seguridad de la información, y las asigna a las personas autorizadas a cargo de las actividades de Tratamiento con el fin de evitar conflictos de interés y de prevenir actividades inapropiadas.

Seguridad en materia de Recursos Humanos

Dispositivos móviles y teletrabajo

Hay una Política de Seguridad para el uso de todos los dispositivos de la Empresa, en particular dispositivos móviles, y se han implantado controles adecuados.

Terminación o cambios en la relación contractual de trabajo

A la terminación del contrato de trabajo de un usuario o en caso de un cambio significativo en su posición dentro de la Empresa, se actualizan de forma inmediata los permisos de acceso, a la vez que las herramientas de trabajo se devuelven y resetean tanto físicamente como en su contenido y programación.

Gestión de los activos

Responsabilidad por los recursos

Todas las herramientas de información se han inventariado y se vigila la asignación de cada uno de ellos a los diversos usuarios responsables. Se ha definido además una Política para su uso correcto.

Clasificación de la información

Toda la información se clasifica y cataloga por los respectivos usuarios en línea con los requisitos de seguridad, así como se procesa adecuadamente.

Gestión de Medios

Toda la información almacenada en los diferentes soportes se clasifica , controla, transfiere y borra de modo que su contenido no se ve comprometido.

Control de accesos

Requisitos empresariales para el control de acceso

Los requisitos organizativos de la Empresa para monitorear el acceso a los recursos de información están documentados en una Política y puestos en práctica mediante procedimientos de acceso. Los accesos a la Red y conexiones están restringidos.

Gestión de acceso de usuario

La asignación de los derechos de acceso de los usuarios se controla desde el registro inicial del usuario hasta la eliminación de los derechos de acceso cuando ya no son necesarios, incluidas las restricciones especiales sobre derechos de acceso privilegiado y la gestión de contraseñas, y está sujeta a comprobaciones y revisiones periódicas, incluida la actualización de los derechos de acceso. En la gestión de los accesos, se aplica el criterio de minimizar los derechos de acceso, ya que éstos se emiten para dar al usuario solamente el acceso a los datos que sea necesario para su trabajo y funciones en el negocio. Los derechos de acceso adicionales requieren autorizaciones específicas.

Responsabilidad del usuario

Los usuarios son conscientes de sus responsabilidades mediante un control de acceso efectivo, por ejemplo, eligiendo una contraseña compleja y manteniéndola confidencial.

Sistemas y aplicaciones para control de acceso

El acceso a la información está sujeto a restricciones de conformidad con la política de control de accesos, mediante un sistema de acceso seguro y administración de contraseñas de acceso, así como mediante el control de utilidades privilegiadas y acceso limitado a todos los códigos fuente.

Cifrado o encriptación

Control criptográfico

Existe una Política sobre encriptación de medios y datos de usuarios. Las autenticaciones están encriptadas.

Seguridad física y del entorno

Hay implementadas medidas de seguridad físicas y de entorno con el fin de prevenir accesos accidentales o ilegítimos, así como la pérdida o la revelación de datos.

Áreas seguras: centro de datos.

Los servicios de la Empresa se prestan desde y alojan en varios centros de datos en diversas partes del mundo. Todos los centros de datos en la cadena de Servicio disponen de sistemas eléctricos, de refrigeración y de red redundantes. Todos los centros de datos tienen detectores de presencia con cámaras de seguridad. Todas las alarmas están concentradas en cuartos de control.

El acceso físico se regula y controla con procedimientos de autorización y reconocimiento.

Equipo

Hay una Política implementada para deshacerse del equipo sobrante, con el fin de destruir de modo seguro toda la información contenida en el mismo.

Seguridad de las Operaciones

Procedimientos y responsabilidades operacionales

Las responsabilidades operativas en IT están documentadas, y se controlan los cambios en las instalaciones y sistemas de IT. Los sistemas de desarrollo, prueba y operativos están separados. Los usuarios están definidos como responsables del correcto funcionamiento de los procedimientos. En su lugar. Es responsabilidad del Cliente de cada servicio individualizado de la Empresa (en adelante, el “cliente”) la gestión de la seguridad lógica de los sistemas operativos y de las aplicaciones instaladas por el cliente..

Protección contra malware

Hay controles activos de virus y malware en los dispositivos de la Compañía, y los usuarios están adecuadamente informados y advertidos.

En cuanto a los servicios de Servidor Virtual y Servidor Dedicado, el cliente es responsable de instalar antivirus y software anti-malware y, si el correspondiente servicio no se ha adquirido, de instalar un firewall.

En cuanto al servicio de alojamiento (hosting), existe una protección en tiempo real instalada en las máquinas.

En cuanto al servicio de correo electrónico, el tráfico de correo se analiza en tiempo real, tanto saliente como entrante, para detectar virus, malware y para la identificación y filtrado de spam. El análisis es automático y se basa en la naturaleza del contenido, en la consulta a bases de datos internacionales, y en la reputación adquirida con base en una serie de parámetros.

Backup

Se hacen y preservan copias de seguridad con la exclusión de servicios para los que el Cliente es responsable de mantener y de gestionar sus propias copias de seguridad (Servidores Dedicados y Virtuales). Para los

servicios de alojamiento y correo, se hacen backups periódicamente, que en el caso del Hosting también pueden ser accedidos por el Cliente. Backups adicionales a los que no tiene acceso el Cliente se hacen regularmente solo con la finalidad de Recuperación de Desastres.

Autenticación y monitorización

Autenticación y sincronización

Todas las actividades y eventos relacionados con la seguridad de la información suceden tras la introducción por parte de los usuarios / administradores de sus claves de autenticación o certificados de identidad. Los relojes de todos los equipos están sincronizados.

Control del software operativo

La instalación del software en los sistemas operativos debe estar controlada y monitorizada.

Seguridad de las comunicaciones

Gestión de seguridad de red

Las redes y los servicios en línea están protegidos, por ejemplo por medio de su separación y segregación.

Transferencia de información

Hay acuerdos vigentes relativos a la transferencia de información de y hacia terceros.

Adquisición, desarrollo y mantenimiento del Sistema

Seguridad en procesos de desarrollo y soporte

Las reglas que rigen la seguridad del software y el desarrollo de sistemas están definidas en una Política. Los cambios en el sistema (tanto para aplicaciones como para sistemas operativos) se controlan siempre. La seguridad de los sistemas se comprueba y se han definido criterios de idoneidad que incluyen aspectos de seguridad.

Relación con los proveedores

Seguridad de la información en la relación con los proveedores

Hay políticas, procedimientos, advertencias, etc. destinadas a proteger el tratamiento de la información de la organización y de clientes que esté accesible a terceros proveedores de IT, así como a otros terceros que forman parte de la cadena de suministro.

Gestión de servicios prestados por el proveedor

La prestación de servicios prestados por proveedores externos se supervisa y verifica / audita en relación con el/los contratos o acuerdos. Se comprueban todos los cambios en el servicio.

Gestión de incidentes en materia de seguridad de la información

Gestión de incidentes de seguridad de la información y mejoras

Hay responsabilidades y procedimientos específicos destinados a gestionar (reportar, asegurar, responder y aprender de) de forma coherente y eficaz los eventos e incidentes relacionados con la seguridad de la información (por ejemplo, el denominado procedimiento de *Violación de Datos*).

Aspectos de seguridad de la información relacionados con la continuidad del negocio

La compañía identifica y documenta sus obligaciones frente a autoridades externas y otros terceros en relación con la seguridad de la información, incluida la propiedad intelectual, documentación contable, e información sobre privacidad.

Revisión de la seguridad de la información

Se revisan de forma periódica los proyectos de la Organización relativos a la seguridad de la información y a las políticas de seguridad, y se aplican medidas correctoras cuando es necesario.

ANEXO 3 (Lista de Sub-encargados)

Se puede obtener la lista de sub – encargados enviando un email a dpo@dada.eu