ACUERDO PARA EL TRATAMIENTO DE DATOS

Anexo II: Acuerdo para el Tratamiento de Datos

Ambas partes, reconociéndose mutuamente la capacidad necesaria para celebrar válidamente el presente contrato,

EXPONEN

PRIMERO.- Que a los efectos del presente contrato se entienden por:

- Datos personales: toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- Interesado: es la persona física identificada o identificable.
- Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, 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.
- Responsable del Tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
- Encargado del Tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable de Tratamiento.
- Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

SEGUNDO. - Que, a los efectos del presente contrato, el Responsable del Tratamiento ha contratado al Encargado del Tratamiento la Licencia de uso de su Software para la gestión del tiempo de sus empleados.

TERCERO. - Que, para la correcta prestación de los servicios relacionados, el Responsable del Tratamiento pondrá a disposición del Encargado del Tratamiento datos de carácter personal automatizados y/o no automatizados que contienen datos personales.

CUARTO. - Que, en cumplimiento de la normativa vigente en Protección de Datos de Carácter Personal, ambas partes acuerdan libremente regular el acceso y tratamiento de los datos de carácter personal mencionados, en base a las siguientes:

CLÁUSULAS

PRIMERA. - Objeto: el tratamiento de los datos de carácter personal que el Responsable de Tratamiento pone a disposición del Encargado del Tratamiento para que este pueda prestar los servicios identificados en el expositivo SEGUNDO.

El tratamiento de los datos personales por parte del Encargado del Tratamiento quedará

circunscrito a lo que resulte necesario para llevar a cabo la prestación de servicios y se efectuará siempre en el marco de esta.

En concreto, los tratamientos a realizar por el Encargado del Tratamiento son:

- Recogida (captura de datos de carácter personal);
- Registro (inscribir o grabar la información en algún sistema o dispositivo, para su posterior tratamiento);
- Conservación (mantener la información durante un determinado periodo de tiempo);
- Consulta (buscar los datos sobre el sistema o dispositivo en el que se encuentra registrada);
- Acceso (posibilidad de conocer los datos mediante su visualización)

En cualquier caso, el encargado del tratamiento no podrá tratar los datos por cuenta del responsable del tratamiento para fines distintos de los especificados en el presente acuerdo.

SEGUNDA. - Duración: el plazo de vigencia del presente contrato se establece en virtud del acuerdo mercantil que se ha formalizado entre ambas partes.

TERCERA. - Finalidad del tratamiento: el acceso por parte del Encargado del Tratamiento a los datos de carácter personal a cargo del Responsable del Tratamiento, será única y exclusivamente para dar cumplimiento a las finalidades relacionadas en el expositivo SEGUNDO.

CUARTA. - El Encargado del Tratamiento podrá acceder a los datos personales de los colectivos de interesados establecidos a continuación:

I. *Datos personales objeto del tratamiento*

Necesarios para la Puesta en Marcha

Nombre, Apellidos, Email Empleado, Cargo, Departamento, Fecha de incorporación, Email del responsable, Email del supervisor, Calendario, Convenio, Horario, Fecha fin de contrato, Oficina.

Opcionales
ID (interno del empleado), DNI, NSS, Cumpleaños, Habilidades, Bolsa Vacaciones. Adicionalmente el Responsable del Tratamiento podrá añadir en concepto de atributos tantos campos como quiera dentro de la ficha del empleado.

De igual modo el Responsable del Tratamiento y sus empleados pueden adjuntar a la plataforma todos aquellos documentos que considere necesarios para su funcionamiento, incluido partes y justificantes médicos.

II. *Colectivos de interesados cuyos datos personales son objeto del tratamiento*

Empleados

QUINTA.- Obligaciones y derechos del Responsable del Tratamiento: según lo establecido en la normativa vigente en Protección de Datos de Carácter Personal el Responsable del Tratamiento deberá:

a) Aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme a la legislación vigente y aplicable.

b) Adoptar las políticas en materia de protección de datos.

c) Garantizar que el Delegado de Protección de Datos o, en su defecto el Responsable de

Privacidad participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

d) Llevar un registro de actividades de tratamiento en caso de tratar datos personales que supongan un riesgo para los derechos y libertades del interesado y/o de manera no ocasional, o que implique el tratamiento de categorías especiales de datos y/o datos relativos a condenas e infracciones.

e) Poner a disposición de los interesados los aspectos esenciales del presente acuerdo.

f) Atender indistintamente los ejercicios de derecho establecidos en la normativa vigente en Protección de Datos de Carácter Personal y cumpliendo las estipulaciones que se indican en la cláusula SÉPTIMA, aunque dicho ejercicio se dirija ante el Encargado del Tratamiento.

g) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado, cuando el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas. Así como realizar consultas previas a la autoridad de control, cuando proceda.

h) Ejercer de forma diligente derecho de información frente al interesado, en el momento de la recogida de los datos.

i) Entregar al encargado del tratamiento los datos a los que se refiere la cláusula CUARTA del presente contrato.

j) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa aplicable y vigente en materia de protección de datos por parte del encargado del tratamiento.

k) Supervisar el tratamiento por parte del encargado del tratamiento.

SEXTA.- Obligaciones y derechos del Encargado del Tratamiento: según lo establecido en la normativa vigente en Protección de Datos de Carácter Personal, el Encargado del Tratamiento y todo su personal deberá:

a) Utilizar los datos personales objeto de tratamiento, en nombre del Responsable del Tratamiento , o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos personales únicamente siguiendo instrucciones del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el Encargado del Tratamiento informará inmediatamente al Responsable del Tratamiento.

c) Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria, así como se hayan comprometido al cumplimiento estricto de las medidas de seguridad previstas para la provisión del servicio previsto en el OBJETO del presente contrato.

d) Garantizar la formación necesaria en materia de protección de datos personales de las

personas autorizadas para tratar datos personales.

e) Tomar todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento. En todo caso, deberá implantar mecanismos para:

a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico, garantizando la recuperación del 99% de la información generada el día del incidente.

c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d. Seudonimizar y cifrar los datos personales, en su caso.

f) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admisibles. El Encargado del Tratamiento puede comunicar los datos a otros encargados del tratamiento del mismo Responsable del Tratamiento, de acuerdo con las instrucciones del Responsable del Tratamiento. En este caso, el Responsable del Tratamiento identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

g) Respetar las condiciones para recurrir a otro Encargado del Tratamiento, según lo establecido en la normativa vigente y aplicable en Protección de Datos de Carácter Personal.

h) Dar apoyo al Responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda. Así como en la realización de las consultas previas a la autoridad de control, cuando proceda.

i) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable, y aceptado expresamente por el Encargado del Tratamiento, en los términos previstos en este acuerdo.

j) Asistir al Responsable del Tratamiento en cuanto a la detección de violaciones de seguridad de los datos, el Encargado del Tratamiento, notificará al Responsable del Tratamiento, sin dilación indebida, con un plazo máximo de 48 Horas a través de correo electrónico a xxx@xxxx.xx ,las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. 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. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

k) Tratar los datos personales puestos a disposición del Encargado de Tratamiento de manera que garantice que el personal a su cargo sigue con las instrucciones del Responsable de Tratamiento.

l) Garantizar que el Delegado de Protección de Datos o, en su defecto el Responsable de Privacidad participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

m) Llevar un registro, en caso de tratar datos personales que supongan un riesgo para los derechos y libertades del interesado o de manera no ocasional, o que implique el tratamiento de categorías especiales de datos y/o datos relativos a condenas e infracciones, de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable.

n) Asistir al Responsable del Tratamiento en cuanto al ejercicio de derechos del interesado y cumpliendo las estipulaciones que se indican en la cláusula SÉPTIMA. Cuando las personas afectadas ejerzan cualquiera de estos derechos frente al Encargado del Tratamiento, relativos a los tratamientos previstos en el objeto del presente contrato, éste debe comunicarlo por correo electrónico a la dirección La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

SÉPTIMA.- Ejercicio de derechos por parte del interesado:

1. Acceso, rectificación, supresión (“Derecho al olvido”) y oposición,
2. Limitación del tratamiento,
3. Portabilidad de datos,
4. A no ser objeto de decisiones individualizadas automatizadas,

Si el interesado dirige alguna solicitud o ejerce alguno de los derechos establecidos en la normativa vigente y aplicable en Protección de Datos de Carácter Personal, el Responsable de Tratamiento, y con el diligente soporte del Encargado de Tratamiento, deberá facilitarle la información sobre las actuaciones solicitadas y realizadas, sin demora y, a más tardar, en el plazo de un mes a partir de la recepción de la solicitud, el cual podrá prorrogarse un máximo de otros dos meses en caso necesario, teniendo en cuenta la complejidad de la solicitud y el número de las solicitudes.

En el mismo sentido, pero en el caso de que el Responsable del Tratamiento y/o el Encargado del Tratamiento no dé curso a la solicitud del interesado, le informará sin demora, y a más tardar al mes de la recepción de la solicitud, de las razones por las que no ha actuado y de la posibilidad de presentar una reclamación ante una Autoridad de Control y de interponer recurso judicial.

La respuesta a la solicitud al ejercicio de derecho se realizará en el mismo formato que haya utilizado el interesado, a menos que solicite que se proceda de otro modo.

OCTAVA. - Transferencia Internacional de Datos: las Transferencias Internacionales de Datos personales sólo podrán realizarse si se cumplen con las exigencias recogidas por la Agencia

Española de Protección de Datos, o cualesquiera otra normativa nacional o comunitaria que las regulen.

Las transferencias de datos personales fuera del Espacio Económico Europeo (EEE) se realizarán únicamente a destinatarios que cuenten con una decisión de adecuación de la Comisión Europea o que ofrezcan garantías adecuadas conforme al RGPD.

En este último caso, las partes acuerdan aplicar las Cláusulas Contractuales Tipo adoptadas por la Comisión Europea mediante la Decisión de Ejecución (UE) 2021/914, que se incorporan como Apéndice 1 al presente Acuerdo.

NOVENA. - Subcontratación: El Encargado del Tratamiento no subcontratará ninguno de los servicios objeto del presente contrato que impliquen el tratamiento de datos personales, salvo los servicios auxiliares que el Encargado del Tratamiento considere necesarios . El Responsable del Tratamiento da su consentimiento general para el uso de subencargados del tratamiento, con sujeción a lo dispuesto en el presente apartado NOVENO.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al Responsable del Tratamiento, con una antelación de 15 días hábiles, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

El Responsable del tratamiento podrá oponerse a ello dentro del plazo concedido. En tal caso, el encargado del tratamiento y el responsable del tratamiento revisarán la documentación que garantice el cumplimiento de la legislación aplicable en materia de privacidad por parte del sub encargado. Si el Responsable del tratamiento sigue oponiéndose a la subcontratación podrá rescindir el acuerdo comercial, siempre que acredite motivos razonables para ello,debido, en particular, a la naturaleza del Software estándar en línea.

La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido. El subcontratista, que también tendrá la condición de Encargado del Tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el responsable. Corresponde al Encargado del Tratamiento inicial regular la nueva relación contractual de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad), previstas en la cláusula SEXTA del presente contrato, y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del sub encargado, el Encargado del Tratamiento inicial seguirá siendo plenamente responsable ante el responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.

A estos efectos se hace constar que Woffu, como ENCARGADO del Tratamiento, mantiene una lista actualizada de subprocesadores disponible en el siguiente Link .

DÉCIMA: Auditoría: El Responsable del Tratamiento podrá llevar a cabo una auditoría al año, como máximo, dentro del horario laboral del Encargado del tratamiento, y tendrá únicamente acceso a aquellas instalaciones directamente relacionadas con la prestación de los servicios. La realización de la auditoría deberá comunicarse con un periodo mínimo de 90 días.

El Responsable del Tratamiento podrá realizar la auditoría mediante un tercero, previa firma de un

acuerdo El Responsable del Tratamiento será responsable de todos los costes de cada auditoría. Toda la información obtenida y derivada de las auditorías será tratada como Información Confidencial.

El Responsable del Tratamiento podrá realizar la auditoría mediante un tercero, previa firma de un acuerdo de confidencialidad aceptable para el Encargado del tratamiento.

En ningún caso el Responsable del Tratamiento podrá requerir, ni el Encargado del tratamiento estará obligado a suministrar información sobre otros proveedores del Encargado del tratamiento o sobre el coste interno de la prestación de los servicios, información privilegiada, interna o confidencial.

El responsable del tratamiento correrá con los gastos derivados de la realización de las auditorías.

Previamente a la realización de la auditoría, el Responsable del Tratamiento deberá acreditar la vigencia de un seguro de responsabilidad civil que cubra, de forma suficiente, los posibles daños y perjuicios que puedan ocasionarse al Encargado del Tratamiento como consecuencia de la auditoría, aportando copia de la póliza y del último recibo de pago.

UNDÉCIMA: Violación de seguridad de los datos: tanto en cuanto exista una instrucción de la autoridad de control, un desarrollo legislativo nacional que regule estas comunicaciones o un acto delegado, en caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento y/o el Encargado de Tratamiento la notificará a la Autoridad de Control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Las violaciones de seguridad que tenga conocimiento el ENCARGADO deberán notificarse, sin dilación indebida y en un máximo de 48 horas, al RESPONSABLE para su conocimiento y aplicación de medidas para remediar y mitigar los efectos ocasionados. No será necesaria la notificación cuando sea improbable que comporte un riesgo para los derechos y las libertades de las personas físicas. La notificación de una violación de seguridad deberá contener, como mínimo, la siguiente información: Descripción de la naturaleza de la violación. Categorías y el número aproximado de interesados afectados. Categorías y el número aproximado de registros de datos afectados. Posibles consecuencias. Medidas adoptadas o propuestas para remediar o mitigar los efectos.

DUODÉCIMA.- Rescisión, resolución y extinción: la rescisión, resolución o extinción de la relación contractual de prestación de servicios entre el Responsable del Tratamiento y el Encargado del Tratamiento, obligará a este último, a petición del Responsable, a la devolución de los soportes y de todos los datos contenidos en los mismos, entregados por parte del Responsable del Tratamiento al Encargado del Tratamiento para la adecuada prestación del servicio, así como todos aquellos datos personales y soportes generados durante la prestación del servicio, serán devueltos al Responsable del Tratamiento en un plazo máximo de 30 días hábiles a contar desde la rescisión del contrato mercantil entre las partes. Esta información será devuelta en el formato en el cual se encuentre en el momento de la resolución del contrato, exceptuando cuando por motivos de volumen requiera un esfuerzo extraordinario por parte del Encargado del Tratamiento, esta situación requerirá un acuerdo entre Responsable del Tratamiento y Encargado del tratamiento a fin de consensuar el formato en el cual se devolverá la información.

La rescisión o extinción de la relación contractual de prestación de servicios obligará al Encargado de Tratamiento a conservar los datos de carácter personal facilitados por el primero, siempre que exista la obligación legal de conservación. Una vez transcurrido el plazo establecido para cubrir las

responsabilidades legales, los datos de carácter personal deberán ser destruidos de forma segura, al igual que cualquier soporte o documento en que conste algún dato de carácter personal. Woffu conservará los datos personales objeto del contrato durante 4 años.

DECIMOTERCERA.- Uso de herramientas de Inteligencia Artificial: Las herramienta, sistema o servicio basado en Inteligencia Artificial utilizado en la ejecución del presente contrato cumplirá con lo dispuesto en el Reglamento (UE) sobre Inteligencia Artificial (AI Act), así como con la normativa vigente en materia de protección de datos personales, ciberseguridad, propiedad intelectual y derechos fundamentales.

El Proveedor se compromete a: (i) emplear únicamente herramientas evaluadas según su nivel de riesgo conforme al AI Act; (ii) mantener registros técnicos y de uso cuando así lo requiera la normativa; (iii) aplicar medidas de supervisión humana adecuadas; (iv) garantizar la transparencia y trazabilidad de los resultados; y (v) no utilizar sistemas prohibidos por la legislación vigente.

En caso de que alguna herramienta deje de cumplir con dichos requisitos, deberá ser sustituida o adaptada de forma inmediata para asegurar la conformidad legal.

DECIMOCUARTA.- Datos de los Intervinientes: Cada una de las partes queda informada de que sus datos de carácter personal serán tratados por la otra parte con la finalidad de permitir el desarrollo, cumplimiento y control de la relación de prestación de servicios concertada, siendo la base del tratamiento dicha relación y conservando los datos durante todo el tiempo en que ésta subsista y aún después, hasta que prescriban las eventuales responsabilidades derivadas de ella. Podrán solicitar el acceso a los datos personales, su rectificación, su supresión, su portabilidad y la limitación de su tratamiento, así como oponerse al mismo, en el domicilio de la otra parte que figura en el encabezamiento. Los datos podrán ser comunicados a las Administraciones Públicas cuando la Ley obligue a ello y a las entidades financieras para la gestión de cobros. Frente a cualquier vulneración de derechos, la parte afectada puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es) u otra autoridad de control.

Para cualquier cuestión relativa al tratamiento de datos personales, por lo que, si lo desea, el RESPONSABLE puede dirigirse a privacy@woffu.com

DECIMOQUINTA. – Legislación aplicable y Jurisdicción: La relación entre las partes se regirá por la normativa vigente y de aplicación en el territorio español. De surgir cualquier controversia las partes podrán acudir a la jurisdicción ordinaria cumpliendo con las normas sobre jurisdicción y competencia al respecto. WOFFU JOB ORGANIZER, S.L tiene su domicilio en BARCELONA,

España. Las cuestiones de responsabilidad entre las partes se regirán por las cláusulas de responsabilidad del acuerdo de servicio entre las partes (Anexo I Licencia de Uso.)

Apéndice I – Cláusulas Contractuales Tipo.

1. Generalidades

1.1. Aplicabilidad. El presente Apéndice– Cláusulas Contractuales Tipo incorpora las cláusulas contractuales tipo (CCT) de la Comisión Europea aplicables a los intercambios de datos personales que impliquen una transferencia de datos personales a un tercer país.

Si alguna de las Partes intercambia datos personales que supongan una transferencia a un país fuera de la UE/EEE sin una decisión de adecuación aplicable, las Partes correspondientes acuerdan que dicha transferencia estará sujeta a las CCT.

1.2. Transferencia. A efectos aclaratorios, "transferencia de datos personales" tiene el significado establecido en el RGPD, según la interpretación del Tribunal de Justicia de la Unión Europea (TJUE) y del Comité Europeo de Protección de Datos (CEPD).

1.3 Subencargados

En caso de que los datos sean transferidos a un subencargado ubicado fuera del EEE, Woffu garantizará que dicho subencargado suscriba las CCT u ofrezca garantías adecuadas equivalentes, conforme a los artículos 28.4 y 46 del RGPD.

2. Cláusulas Contractuales Tipo.

2.1 Módulo aplicable

Se aplicará el Módulo 2 (transferencia de Responsable a Encargado).

2.2 Opciones acordadas entre las partes

- Cláusula 7: Aplicable.
- Cláusula 9: Se aplica la Opción 2 (autorización general para el uso de subencargados), conforme a lo establecido en la cláusula NOVENA del DPA. El plazo de notificación será de 15 días hábiles.
- Cláusula 11: La redacción opcional no se incluye.
- Cláusula 17: La legislación aplicable será la de España, al tratarse de un Estado miembro de la Unión Europea que reconoce los derechos de los terceros beneficiarios conforme al RGPD.
- Cláusula 18: Cualquier controversia derivada de estas cláusulas se resolverá judicialmente en España, ante los tribunales de Barcelona. Las partes se someten expresamente a dicha jurisdicción, sin perjuicio del derecho de los interesados a ejercer acciones legales en el Estado miembro donde residan habitualmente.

2.3. **Anexo I de Cláusulas tipo de la Comisión Europea (CCT)** . La información contenida en el Anexo I de Cláusulas tipo de la Comisión Europea (CCT) se complementa con el Anexo II del presente documento correspondiente al Acuerdo para el tratamiento de datos pactado entre las Partes.

2.4. **Anexo II de Cláusulas tipo de la Comisión Europea (CCT)** . Las medidas técnicas y organizativas aplicables, incluidas las que garantizan la seguridad de los datos, se establecen en el Anexo III del presente documento correspondiente MEDIDAS TÉCNICAS DE SEGURIDAD.

2.5. **Anexo III de Cláusulas tipo de la Comisión Europea (CCT)** . Los subencargados del tratamiento quedan enumerados en la cláusula Novena “Subcontratación” del Acuerdo de Tratamiento de datos previsto en el presente documento.

ANEXO III MEDIDAS TÉCNICAS

Woffu es un software as a service que ofrece acceso a la Woffu Saas Platform, desarrollada utilizando todo el conocimiento y la experiencia adquirida con clientes con diferentes casuísticas durante los últimos años.

El servicio de hosting y conectividad de Woffu es Azure Cloud, un conjunto de servicios en la nube de la empresa Microsoft, que nos garantiza un almacenamiento y backup seguro y nos proporciona toda la accesibilidad de un entorno cloud.

Azure Cloud cuenta con Centros de Datos propios ubicados en Europa. En el caso de Woffu, todos los datos se replican y se respaldan entre dos regiones de Microsoft, al Norte (Irlanda) y al Este (Países Bajos). De esta forma aseguramos que ante una eventual caída de una región, desde Woffu podemos seguir ofreciendo servicio a nuestros clientes sin interrupciones.

Uno de los beneficios de que Woffu sea una SaaS nativa es que todos los datos de la empresa están ubicados en la nube, lo que hace que sea bastante fácil mantener las copias de seguridad actualizadas y escalar la plataforma cuando sea necesario.

Certificaciones ISO/IEC - Certificado de Privacidad en la Nube

Las certificaciones forman parte del día a día. En Woffu nos esforzamos arduamente para alcanzar los más altos estándares de seguridad para nuestros clientes. La Organización Internacional de Normalización (ISO) es una organización independiente y no gubernamental, y el desarrollador más grande del mundo de estándares internacionales voluntarios. Por otro lado, la Comisión Electrotécnica Internacional (IEC) es la organización líder del mundo en la preparación y publicación de normas internacionales acerca de tecnologías eléctricas, electrónicas y relacionadas.

Sabiendo la importancia y valor de estas organizaciones, hemos conseguido 3 certificaciones ISO/IEC que garantizan nuestro compromiso con la privacidad de datos y procesos.

ISO/IEC 27001. Certificación en la Gestión de la Seguridad de la Información.

La información de nuestros clientes es importante para nosotros por lo que es de vital importancia contar con un Sistema de Gestión de la Seguridad de la Información (SGSI) que nos permita la gestión y control de los riesgos de la seguridad de la información.

La certificación ISO/IEC 27001 nos permite contar con un SGSI basado en las mejores prácticas y para asegurarnos de tener control de dicho sistema en Woffu hemos implementado los 114 controles de la ISO/IEC 27002.

ISO/IEC 27018. Certificación en la Seguridad y Protección de información personal en la nube.

No todos los datos se tratan de la misma manera, dependiendo del tipo de dato que se maneja se deben de tener controles para protegerla.

La norma ISO/IEC 27018 nos permite tener un marco de privacidad enfocado a la seguridad de la información y proteger de la mejor manera la información de identificación personal (PII-Personally Identifiable Information) en un sistema en la nube como es Woffu.

ISO/IEC 27701. Certificación en la Protección de la información de Identificación Personal (PII-Personally Identifiable Information).

Dar cumplimiento al RGPD es de vital importancia para Woffu y por eso estamos certificados en ISO/IEC 27701 ya que esta norma es una integración de la norma 27001 y los requerimientos esenciales del RGPD.

Haber obtenido dichas certificaciones significa una apuesta por parte de Woffu por la seguridad de la información que ostenta. Es esencial proteger la información, principalmente la de Identificación Personal (PII) en la nube de sus clientes y de sus empleados. La certificación convierte a Woffu en uno de los primeros SaaS especializado en RRHH de España en obtener los distintivos. De esta manera aportamos una mayor solvencia para nuestros clientes porque tienen la certeza de que su información y la de sus personas estará protegida.

Reglamento General de Protección de Datos (RGPD)

La confianza de nuestros clientes es vital para una buena relación y un buen desempeño de sus actividades diarias. No solo alcanzamos las certificaciones ISO/IEC, sino también cumplimos con el RGPD, la nueva legislación de carácter europeo de protección de datos de los clientes que se complementa con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Políticas, normas y medidas para el cumplimiento al Reglamento General de Protección de Datos

La Certificación ISO/IEC 27701 nos ha ayudado a mejorar los procesos de Protección de Datos de todos nuestros clientes y sus usuarios. A partir de aquí, en Woffu buscamos proteger el intercambio de información con terceras personas, estas son algunas de las políticas normas y medidas que hemos establecido para asegurar la integridad, disponibilidad y confidencialidad de los datos:

- Acuerdo de Confidencialidad con terceros para prevenir la divulgación no autorizada de la información.
- Compromiso de Confidencialidad y Secreto con todos los empleados para prevenir la divulgación no autorizada de la información.
- Solicitud y revisión de los antecedentes penales de las personas que tienen acceso a los datos personales.
- El acceso a los datos de los clientes es restringido y únicamente pueden acceder a ellos el personal autorizado y con la finalidad de dar soporte al cliente.
- Transferencia de datos con infraestructura:
  - Solo se permiten conexiones encriptadas a la base de datos SQL Azure.
  - Solo se permiten conexiones seguras a los servicios de almacenamiento y al servicio de caché.
  - La transferencia de archivos con terceros es cifrada mediante el protocolo SFTP.

Requisitos Generales de IT

Woffu es una aplicación web por lo que es imprescindible la conexión a la red. Para ordenadores de sobremesa o portátiles, Woffu está optimizado para las últimas versiones de Google Chrome (Versión 84 o superior), Firefox (Versión 79 o superior), y Edge (Versión 80 o superior) con versiones de Windows 7 o superior y Safari (Versión 12) con versiones de MacOS 10.12 o superior.

Para dispositivos portátiles, como móviles y tablets, la navegación es a través de sus navegadores web dada la versión responsive o con la aplicación móvil de Woffu disponible para iOS (Versión 11.0 o superior) y Android (Versión 5.0 o superior).

En Woffu estamos comprometidos en alcanzar los estándares más altos de seguridad para cuidar de la información de tu empresa y de tu gente. Por eso hemos alcanzado las 3 ISO/IEC siendo una de las primeras SaaS en España en obtenerlas.

Descripción de las medidas de seguridad técnicas y organizativas aplicadas por WOFFU JOB ORGANIZER SL

Con el fin de garantizar la seguridad de la información a la que accede, procesa, transmite y almacena Woffu Job Organizer SL., como encargado del tratamiento durante la prestación de servicios al responsable, Woffu garantizará, el cumplimiento de los siguientes requisitos de seguridad:

- Implementar una Política de Seguridad conforme a la normativa aplicable y a las internacionales como NIST o ISO 27001, cuyo alcance deberá abarcar a toda la empresa y, en todo caso, deberá cubrir el servicio objeto del contrato.
- Disponer de un Plan de Negocio actualizado, garantizando que se compruebe periódicamente y que cubra el alcance de los servicios prestados.
- Disponer de un Plan de Recuperación de Desastres actualizado, garantizando que se compruebe periódicamente y que cubra el alcance de los servicios prestados.
- Garantizar que los equipos cuenten con software antimalware con firmas actualizadas en todo momento.
- Garantizar que se dispone de elementos para proteger a los usuarios de correos electrónicos de suplantación de identidad, robo de identidad o programas maliciosos.
- Garantizar que se aplican parámetros de seguridad a los servidores o equipos que nos dan servicio.
- Garantizar que los empleados que van a dar servicio han participado en campañas de ciberseguridad durante el último año y también es deseable que hayan recibido formación.
- Garantizar que la aplicación o servicio objeto del contrato ha sido desarrollado siguiendo prácticas de programación seguras y que se han realizado Penetration Tests o ejercicios Red Team realizados.
- Disponer de un proceso de respuesta ante incidentes que garantice una adecuada gestión y coordinación de recursos para mitigar los efectos del incidente y favorezca la interrupción del servicio en caso de un incidente o la vuelta a la normalidad.
- Garantizar que la información tratada relativa al servicio se almacena y transmite cifrada.
- Garantizar que la Información Personal cumple con la normativa vigente.
- Implementar medidas sobre el Acceso físico y Lógico.
- Disponer de Controles de Separación de Datos a nivel de base de datos, indicando
- en cada registro a qué empresa pertenecen y estableciendo controles a nivel de lógica de negocio según el usuario autenticado usuario.

- Contar con un proceso de auditoría interna y que esta se realice anualmente.
- Contar con compromiso de Subprocesadores.
- Contar con una Política y Programa de protección de datos personales que le permita cumplir con la obligación exigida por la legislación aplicable.
- Disponer de un Programa de Gestión de Incidencias.

El Cliente podrá exigir, previo aviso, que se demuestre el cumplimiento con las obligaciones especificadas en este documento.