Contrato de Tratamiento de Datos

Versión del 17.10.2025

El presente Contrato de Tratamiento de Datos («**DPA**»), forma parte del contrato, en lo sucesivo, el «**Contrato**», que suscriben OVH Hispano SL «**OVHcloud**») y el Cliente, y que recoge los términos y condiciones aplicables a los servicios prestados por OVHcloud (los «**Servicios**»). El presente DPA y el resto de cláusulas del Contrato se indican a título complementario. Sin embargo, en caso de conflicto, el DPA prevalecerá.

El significado de los términos que comienzan por mayúscula y que no se definen en este DPA se corresponderá con el significado establecido en el Contrato. Los términos "Interesado", "Normas Corporativas Vinculantes", "Responsable del Tratamiento", "Dato Personal", "Incumplimiento de la seguridad de los Datos Personales", "Tratamiento de Datos Personales", "Encargado del Tratamiento", "Autoridad de Control" se interpretarán como lo definido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ("**Reglamento General de Protección de Datos**" o "**RGPD**").

Este DPA, tiene por objeto, de conformidad con el artículo 28 del RGPD, establecer las condiciones en las que OVHcloud, como Encargado del Tratamiento y como parte de los Servicios recogidos en el Contrato, para llevar a cabo el tratamiento de Datos Personales en nombre del Cliente y siguiendo instrucciones de este, excluyendo las actividades de tratamiento de datos personales ejecutadas por OVHcloud como responsable del tratamiento. Las condiciones en que OVHcloud trata, como Responsable del Tratamiento, Datos Personales relativos al Cliente (incluidos los agentes del Cliente), se definen en la Política de Uso de Datos de OVHcloud.

A efectos de este DPA, el Cliente puede actuar tanto como "**Responsable del Tratamiento**" o como "**Encargado del Tratamiento**" en lo que concierne a los Datos Personales. En caso de que el Cliente actúe como encargado del tratamiento por cuenta de un responsable del tratamiento tercero, las Partes acuerdan expresamente las siguientes condiciones:

(a) el Cliente garantizará (i) que el Responsable del Tratamiento haya concedido todas las autorizaciones necesarias para celebrar este DPA, incluido el nombramiento de OVHcloud como subencargado del tratamiento por parte del Cliente; (ii) que, de conformidad con el artículo 28 del RGPD, se haya celebrado un contrato con el Responsable del Tratamiento que se ajuste plenamente a los términos y condiciones del Contrato, incluyendo este DPA; (iii) que cualquier instrucción que OVHcloud reciba por parte del Cliente en aplicación del Contrato y de este DPA se ajuste plenamente a las instrucciones del Responsable del Tratamiento; y (iv) que toda la información que OVHcloud comunique o facilite de conformidad con este DPA sea debidamente comunicada al Responsable del Tratamiento cuando sea necesario;

(b) OVHcloud (i) solo tratará Datos Personales siguiendo instrucciones del Cliente y (ii) no recibirá ninguna instrucción directamente del Responsable del Tratamiento, excepto en aquellos casos en los que el Cliente haya desaparecido *de facto* o haya dejado de existir jurídicamente sin que ninguna entidad sucesora haya asumido los derechos y obligaciones del Cliente;

(c) El Cliente, que es plenamente responsable ante OVHcloud de la correcta ejecución de sus obligaciones como Responsable del Tratamiento según lo dispuesto en este DPA, deberá indemnizar y eximir a OVHcloud de toda responsabilidad en caso de (i) incumplimiento por parte del Responsable del Tratamiento de la legislación aplicable o de (ii) cualquier acción, requerimiento o reclamación por parte del Responsable del Tratamiento en relación con las disposiciones del Contrato (incluido este DPA) o con cualquier instrucción que OVHcloud haya recibido del Cliente.

1. Ámbito de aplicación

1.1 OVHcloud, en su calidad de Encargado del Tratamiento que actúa siguiendo las instrucciones del Cliente, está autorizada a tratar los Datos Personales del Responsable del Tratamiento en la medida en que sea necesario para prestar los Servicios.

1.2 La naturaleza de las operaciones realizadas por OVHcloud en materia de Datos Personales puede enmarcarse en el ámbito de la informática, el almacenamiento o cualquier otro Servicio similar tal y como se describe en el Contrato.

1.3 El Cliente determina y controla, a su total discreción, el tipo de Datos Personales y las categorías de Interesados.

1.4 OVHcloud realiza las actividades de tratamiento durante el período previsto en el Contrato.

2. Selección de los Servicios

2.1 El Cliente, que es el único responsable de la selección de los Servicios, deberá asegurarse de que los Servicios seleccionados posean las características y condiciones necesarias con relación a las actividades y los fines del tratamiento del Responsable del Tratamiento, así como al tipo de Datos Personales tratados en el marco de los Servicios, especialmente cuando los Servicios sean utilizados para tratar Datos Personales sujetos a reglamentación o normas específicas (por ejemplo, datos de salud o bancarios en determinados países). El Cliente es conocedor de que OVHcloud ofrece determinados Servicios que disponen de medidas organizativas y de seguridad específicamente diseñadas para el tratamiento de datos sanitarios o bancarios.

2.2 En caso de que el tratamiento del Responsable del Tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, el Cliente deberá seleccionar cuidadosamente sus Servicios. A la hora de evaluar el riesgo, se deben tener en cuenta principalmente, pero no de manera exhaustiva, los siguientes criterios: evaluación o calificación de los Interesados; decisiones automatizada con efectos jurídicos o similares significativos; seguimiento sistemático de los Interesados; tratamiento de datos sensibles o datos de carácter personal especialmente protegidos; tratamiento a gran escala; comparación o combinación de conjuntos de datos; tratamiento de datos referentes a Interesados vulnerables; uso de nuevas tecnologías innovadoras desconocidas por el público para el tratamiento.

2.3 OVHcloud deberá proporcionar al Cliente información, en las condiciones establecidas en la sección «Auditoría», sobre las medidas de seguridad implementadas en el marco de los Servicios, en la medida en que sea necesario para evaluar la conformidad de dichas medidas con respecto a las actividades de tratamiento del Responsable del Tratamiento.

3. Conformidad con la Regulación Aplicable

Las Partes deberán respetar las disposiciones reglamentarias aplicables en materia de protección de datos, incluyendo el Reglamento General de Protección De Datos.

4. Obligaciones de OVHcloud

4.1 OVHcloud se compromete a:

a) tratar los Datos Personales cargados, almacenados y utilizados por el Cliente en el marco de los Servicios solo en la medida necesaria y proporcionada para prestar los Servicios con arreglo al Contrato;
b) no acceder ni utilizar los Datos Personales con fines distintos a los necesarios para la correcta ejecución de los Servicios (en particular, en relación con la gestión de Incidencias);
c) implementar las medidas técnicas y organizativas descritas en el Contrato para garantizar la seguridad de los Datos Personales en el marco del Servicio;
d) garantizar que los trabajadores de OVHcloud autorizados a tratar Datos Personales en el marco del Contrato estén sujetos a obligaciones de confidencialidad y reciban la formación adecuada en materia de protección de Datos Personales;

e) informar al Cliente si, en su opinión y basándose en la información de la que disponga, una instrucción del Cliente infringe el RGPD u otras disposiciones en materia de protección de datos de la Unión Europea o de los Estados Miembros de la Unión Europea.

4.2 En caso de recibir alguna solicitud por parte de autoridades judiciales, administrativas o de otro tipo para obtener la comunicación de Datos Personales tratados por OVHcloud en virtud de este DPA, OVHcloud hará todo lo posible para (i) analizar la competencia de la autoridad requirente y la validez de la solicitud; (ii) responder únicamente a autoridades y solicitudes que no sean obviamente incompetentes o inválidas; (iii) limitar la comunicación de los datos solicitados por la autoridad; e (iv) informar de antemano al Cliente (salvo que esté prohibido por la ley aplicable).

4.3 En caso de que la solicitud provenga de una autoridad que no sea europea para obtener la comunicación de datos personales tratados por OVHcloud en virtud de este DPA en nombre de un Cliente europeo, OVHcloud se opondrá a la solicitud, con sujeción a los siguientes casos:

(x) la solicitud se realiza de conformidad con un acuerdo internacional, como, por ejemplo, un tratado de asistencia judicial mutua, vigente entre el país requirente y la Unión Europea o el Estado miembro donde se encuentra el dato personal o el Estado miembro de la entidad de OVHcloud en la que el cliente tiene registrada su cuenta de cliente de OVHcloud;
(y) los Datos Personales solicitados están almacenados en un centro de datos ubicado fuera de la Unión Europea;
(z) la solicitud se presenta de conformidad con el artículo 49 del RGPD, persigue en particular una razón importante de interés público reconocida por el derecho de la Unión o de los Estados miembros de la Unión Europea o es necesaria para salvaguardar los intereses vitales del interesado u otras personas.

4.4 A petición escrita del Cliente, OVHcloud proporcionará al Cliente la asistencia razonable sobre la realización de evaluaciones de impacto relativas a la protección de datos y sobre consultas a la autoridad de control competente, en caso de que así se lo exija al Cliente la legislación aplicable en materia de protección de datos, y solo en la medida en que dicha asistencia sea necesaria y se refiera al tratamiento de Datos Personales por parte de OVHcloud. Dicha asistencia consistirá en ofrecer información sobre las medidas de seguridad adoptadas por OVHcloud en sus Servicios.

4.5 OVHcloud se compromete a adoptar las siguientes medidas técnicas y organizativas:

(a) medidas de seguridad física destinadas a impedir el acceso de personas no autorizadas a la Infraestructura en la que se almacenan los datos del Cliente;
(b) controles de identidad y de acceso mediante un sistema de autenticación, así como una política de contraseñas;
(c) un sistema de gestión de acceso que permita limitar el acceso a las instalaciones exclusivamente a las personas que necesiten acceder a ellas en el marco de sus funciones y de su ámbito de responsabilidad;
(d) personal de seguridad encargado de velar por la seguridad física de las instalaciones de OVHcloud;
(e) un sistema de aislamiento físico y lógico de los clientes entre sí;
(f) procedimientos de autenticación de los usuarios y administradores, así como medidas de protección del acceso a las funciones de administración;
(g) un sistema de gestión de acceso para las operaciones de soporte y mantenimiento donde apliquen los principios de mínimo privilegio y necesidad de conocimiento; y
(h) procesos y medidas que permitan rastrear todas las acciones realizadas en su sistema de información.

4.6 Estas medidas técnicas y organizativas están expuestas con mayor detalle en el Sitio Web de OVHcloud.

5. Incumplimiento de la Seguridad de los Datos Personales

5.1 En caso de que OVHcloud tuviese conocimiento de cualquier incidencia que pudiera afectar a los Datos Personales del Responsable del Tratamiento (tales como el acceso, la pérdida, la comunicación o la alteración

de datos sin autorización), OVHcloud deberá informar al Cliente sin dilación indebida.

5.2 Dicha notificación deberá (i) describir la naturaleza de la incidencia; (ii) describir las posibles consecuencias de la incidencia; (iii) especificar las medidas adoptadas o propuestas por OVHcloud en respuesta a la incidencia; e (iv) indicar una persona de contacto en OVHcloud.

6. Localización y Transferencia de Datos Personales

6.1 Cuando un Servicio permita al Cliente almacenar Contenido y, en concreto, Datos Personales, la localización o localizaciones, la zona geográfica en la que se encuentre el Centro o Centros de Datos disponibles se especifica en el Sitio Web de OVHcloud. Cuando haya varias localizaciones o zonas geográficas disponibles, el Cliente deberá elegir la o las que prefiera al realizar el Pedido. Sin perjuicio de cualquier disposición en contrario establecida en las Condiciones Particulares del Servicio aplicables, OVHcloud no modifica, sin la aprobación previa del Cliente, la localización o zona geográfica seleccionada al realizar el Pedido.

6.2 Sin perjuicio de lo anterior relativo a la localización de los Centros de Datos, OVHcloud y los Subencargados del Tratamiento autorizados de conformidad con la sección 7 siguiente podrán tratar a distancia el Contenido del Cliente, siempre que las operaciones de tratamiento se produzcan cuando sea necesario para la correcta ejecución de los Servicios y, en particular, en relación con los fines de seguridad y mantenimiento del Servicio.

6.3 Respecto al uso de los Servicios ubicados en Centros de Datos que no estén ubicados en Europa, (a) los Centros de Datos podrán estar ubicados en Países que no estén sujetos a una decisión de adecuación de la Comisión Europea de conformidad con el artículo 45 del RGPD ("Decisión de Adecuación") o (b) el Contenido de Cliente, de acuerdo con las secciones 6.2 y 7 de este DPA, podrá ser tratado por dichos países no sujetos a una Decisión de Adecuación.

6.4. En caso de que el Cliente utilice los Servicios mencionados en el párrafo anterior con el fin de procesar Datos Personales sujetos al RGPD, el Cliente será considerado como Responsable del Tratamiento de Datos; OVHcloud será considerada como encargada del tratamiento de datos y sus filiales, como subencargadas. Cuando se transfieran datos personales a filiales en países en los que no se haya adoptado una Decisión de Adecuación, OVHcloud será considerada como Exportadora de Datos y sus filiales como Importadoras de Datos conforme al RGPD. En este contexto, OVHcloud y sus filiales han suscrito cláusulas contractuales tipo adoptadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión Europea de 4 de junio de 2021 (en lo sucesivo, «Cláusulas Contractuales Tipo»), que figuran anexas a este DPA, aplicables a las transferencias mencionadas.

6.5. Para Servicios ubicados en centros de datos situados dentro de la Unión Europea, si las Condiciones de Servicio aplicables establecen que el tratamiento de Datos Personales sujetos a este DPA puede realizarse desde uno o más países en los que no se haya adoptado una Decisión de Adecuación, se aplicarán los Cláusulas Contractuales Tipo anteriormente mencionadas.

6.6. En caso de aplicación de las Cláusulas Contractuales Tipo de conformidad con las cláusulas 6.3, 6.4 y 6.5 de este DPA, el Cliente será responsable de (i) evaluar la eficacia de las Cláusulas Contractuales Tipo (incluyendo las medidas técnicas y organizativas correspondientes), teniendo en cuenta en particular las categorías de datos que el Cliente pretende tratar como parte de los Servicios, así como las legislaciones y prácticas de los países receptores, con el fin de determinar si existe algún elemento en dichas legislaciones o prácticas que pudiera menoscabar la eficacia de las Cláusulas Contractuales Tipo, y (ii), en caso de que la evaluación revele que las Cláusulas Contractuales Tipo no son efectivas, implementar, tal como recomienda el Comité Europeo de Protección de Datos, medidas complementarias destinadas a garantizar un nivel de protección equivalente en lo esencial al garantizado en la Unión Europea. OVHcloud se compromete a ayudar al Cliente proporcionando, previa solicitud, cualquier información en su posesión que pudiera ser útil para la evaluación del Cliente. Asimismo, el Cliente será responsable de realizar cualquier diligencia u obtener cualquier autorización o consentimiento que pudieran, en su caso, ser requeridos para permitir la transferencia de Datos Personales a países en los que no se haya adoptado una Decisión de Adecuación.

6.7 Cualquier Cláusula Contractual Tipo deberá complementarse con otras Condiciones de Servicios

aplicables (incluido este DPA) que se aplicará *mutatis mutandis* tanto al Importador o Importadores de los Datos como al Exportador o Exportadores de los Datos, siempre que no entren en conflicto con las Cláusulas Contractuales Tipo. En caso de conflicto, prevalecerán las Cláusulas Contractuales Tipo.

7. Subencargados del Tratamiento

7.1 De conformidad con lo dispuesto en la sección «Localización y transferencia de Datos Personales» del presente Contrato, OVHcloud está autorizado a licenciar subcontratistas para que le asistan en el marco de la ejecución de los Servicios. En el marco de esta asistencia, los subcontratistas podrán participar en las actividades de tratamiento de datos realizadas por OVHcloud bajo las instrucciones de los Clientes.

7.2 La lista de los subcontratistas autorizados a participar en las actividades de tratamiento realizadas por OVHcloud bajo las instrucciones del Cliente ("**Subencargado(s) del Tratamiento**"), incluidos los Servicios en cuestión y el lugar desde el cual pueden tratar los Datos Personales del Cliente de conformidad con el presente Contrato, figura (a) en el Sitio Web de OVHcloud o, (b) en las correspondientes Condiciones Particulares aplicables, en caso de que un Subencargado del Tratamiento participe únicamente en un Servicio específico.

7.3 Si OVHcloud decidiese cambiar un Subencargado del Tratamiento o incorporar a un nuevo Subencargado del Tratamiento ("**Cambio de Subencargado del Tratamiento**"), OVHcloud notificará al Cliente en su panel de control o por correo electrónico (a la dirección de correo electrónico registrada en la Cuenta del Cliente) (a) con treinta (30) días de antelación si el Subencargado del Tratamiento fuese una Filial de OVHcloud ubicada en la Unión Europea o en un país que esté sujeto a una Decisión de Adecuación; o (b) con noventa (90) días de antelación en cualquier otro caso. El Cliente tiene derecho a oponerse a un Cambio de Subencargado del Tratamiento de acuerdo con lo establecido en el RGPD. Tal oposición será notificada a OVHcloud dentro de los quince (15) días siguientes a la notificación de Cambio de Subencargado del Tratamiento por parte de OVHcloud al Cliente, en ella se deberá especificar la razón de la oposición. Esta oposición será notificada por el Cliente a través de su Interfaz de Gestión utilizando la categoría "Solicitud de Protección de Datos" o por escrito al *Delegado de Protección de Datos, OVH SAS, 2 rue Kellermann 59100 Roubaix (Francia)*. OVHcloud no estará obligada en ningún caso a renunciar a un Cambio de Subencargado del Tratamiento. Si a raíz de una oposición del Cliente, OVHcloud no renuncia al Cambio de Subencargado del Tratamiento, el Cliente tiene derecho a rescindir los Servicios afectados.

7.4 OVHcloud garantizará que cualquier Subencargado del Tratamiento sea, como mínimo, capaz de cumplir las obligaciones contraídas por OVHcloud, en virtud del presente DPA, relativas al tratamiento de Datos Personales realizado por el Subencargado del Tratamiento. A tal efecto, OVHcloud deberá celebrar un contrato con el Subencargado del Tratamiento. OVHcloud seguirá siendo plenamente responsable ante el Cliente en caso de incumplimiento de dichas obligaciones por parte del Subencargado del Tratamiento.

7.5 OVHcloud queda autorizada a recurrir a proveedores terceros (tales como proveedores de energía, proveedores de red, gestores de puntos de conexión de red o de centros de datos en la modalidad de housing, proveedores de hardware y software, transportistas, proveedores de servicios técnicos, vigilancia, etc.), independientemente de donde se encuentren, sin tener que informar al Cliente ni solicitar su consentimiento previo, en la medida que dichos proveedores terceros no lleven a cabo un tratamiento de los Datos Personales del Cliente.

8. Obligaciones del Cliente

8.1 Para el tratamiento de Datos Personales según lo dispuesto en el Contrato, el Cliente deberá proporcionar a OVHcloud por escrito (a) cualquier instrucción pertinente y (b) cualquier información necesaria para la elaboración de los registros de las actividades de tratamiento por parte del Encargado del Tratamiento. El Cliente es el único responsable de dicho tratamiento de información y de las instrucciones proporcionadas a OVHcloud.

8.2 El Cliente es responsable de garantizar:

a) que el tratamiento de los Datos Personales del Cliente en el marco de ejecución del Servicio tenga una base jurídica adecuada (p. Ej., consentimiento del Interesado, consentimiento del Responsable del Tratamiento, intereses legítimos, autorización por parte de la autoridad de control pertinente, etc.);
b) que se hayan realizado todos los procedimientos y trámites necesarios (como evaluaciones de impacto referentes a la protección de datos, notificaciones y solicitudes de autorización a la autoridad competente en materia de protección de datos o a cualquier otro organismo competente, en caso necesario);
c) que los Interesados estén informados del tratamiento de sus Datos Personales de forma concisa, transparente, comprensible y de fácil acceso, con un lenguaje claro y sencillo según lo dispuesto en el RGPD, y
d) que los Interesados sean informados de sus derechos y tengan en todo momento la posibilidad de ejercer dichos derechos según lo dispuesto en el RGPD de forma directa con el Responsable del Tratamiento.

8.3 El Cliente es responsable de aplicar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los recursos, sistemas, aplicaciones y operaciones que no entren dentro del ámbito de responsabilidad de OVHcloud, tal y como se define en el Contrato (en particular, cualquier sistema o software desplegado o ejecutado por el Cliente o los Usuarios en el marco de los Servicios).

9. Derechos del Interesado

9.1 El Responsable del Tratamiento es plenamente responsable de informar a los Interesados de sus derechos, así como de respetar dichos derechos, incluidos los derechos de acceso, rectificación, supresión, limitación, portabilidad u oposición.

9.2 OVHcloud deberá proporcionar la asistencia y la cooperación necesarias que se le puedan exigir razonablemente para responder a las solicitudes del Interesado. Dichas asistencia y cooperación consistirán en (a) informar al Cliente de cualquier solicitud que reciba directamente por parte del Interesado y (b) permitir que el Responsable del Tratamiento diseñe y despliegue las medidas técnicas y organizativas necesarias para responder a las solicitudes del Interesado. El Responsable del Tratamiento será el único responsable de responder a dichas solicitudes.

9.3 El Cliente reconoce y acepta que, en caso de que dicha asistencia y cooperación obliguen al Encargado del Tratamiento a aportar cuantiosos recursos, dicho gasto podrá ser facturado tras previo aviso y acuerdo con el Cliente.

10. Supresión y Devolución de los Datos Personales

10.1 En caso de expiración de un Servicio (en particular, en caso de rescisión o no renovación), OVHcloud se compromete a suprimir, en las condiciones previstas en el Contrato, todo el Contenido (incluidos información, datos, archivos, sistemas, aplicaciones, sitios web y otros elementos) reproducido, almacenado, alojado o utilizado de cualquier otra forma por el Cliente en el marco de los Servicios, a menos que un requerimiento emitido por una autoridad legal o judicial competente o la legislación aplicable de la Unión Europea o de un Estado Miembro de la Unión Europea dispongan lo contrario.

10.2 El Cliente es el único responsable de garantizar que se realizan las operaciones necesarias (copia de seguridad, transferencia a una solución de terceros, capturas de pantalla, etc.) para la conservación de los Datos Personales, en particular antes de la rescisión o la expiración de los Servicios, y antes de proceder a realizar cualquier operación de supresión, actualización o reinstalación de los Servicios.

10.3 A este respecto, se informa al Cliente de que la rescisión y la expiración de un Servicio por cualquier motivo (incluida, sin carácter exhaustivo, la no renovación), así como la realización de determinadas operaciones para actualizar o reinstalar los Servicios, podrían implicar automáticamente la supresión irreversible de todo el Contenido (incluidos información, datos, archivos, sistemas, aplicaciones, sitios web y

otros elementos) reproducido, almacenado, alojado o utilizado de cualquier otra forma por el Cliente en el marco de los Servicios, incluida cualquier posible copia de seguridad.

11. Responsabilidad

11.1 OVHcloud solo será responsable de los daños provocados por el tratamiento en aquellos casos en los que (i) no haya cumplido con las obligaciones del RGPD relativas específicamente a los encargados del tratamiento o (ii) haya actuado de forma contraria a las instrucciones lícitas por escrito del Cliente. En tales casos, se aplicará la disposición sobre responsabilidad del Contrato.

11.2 En caso de que OVHcloud y el Cliente participen, según lo dispuesto en este Contrato, en un proceso de tratamiento que pudiera provocar daños al Interesado, el Cliente deberá, en un primer momento, asumir la indemnización íntegra (o cualquier otra compensación) debida al Interesado y, a continuación, reclamar a OVHcloud la parte proporcional de la compensación correspondiente a la parte de responsabilidad de OVHcloud por dichas pérdidas, siempre y cuando se apliquen cualquier limitación de responsabilidad según lo dispuesto en el Contrato.

12. Auditorías

12.1 OVHcloud deberá proporcionar al Cliente toda la información necesaria para (i) acreditar el cumplimiento de las obligaciones establecidas en el RGPD y (ii) permitir que se realicen auditorías. Dicha información está disponible en la documentación estándar del Sitio Web de OVHcloud. El Cliente podrá recibir información adicional, previa solicitud al Soporte de OVHcloud.

12.2 Si un Servicio cuenta con una certificación, cumple con un código de conducta o está sujeto a procedimientos de auditoría específicos, OVHcloud pondrá a disposición del Cliente, previa solicitud por escrito, los correspondientes certificados e informes de auditoría.

12.3 En caso de que dicha información, incluyendo los mencionados certificados e informes de auditoría, resulte insuficiente para permitir que el Cliente demuestre que cumple con las obligaciones establecidas en el RGPD, OVHcloud y el Cliente deberán acordar las condiciones operativas, financieras y de seguridad para una inspección técnica *in situ*. Las condiciones de esta inspección no deben, bajo ninguna circunstancia, afectar a la seguridad de otros clientes de OVHcloud.

12.4 Dicha inspección *in situ*, así como la comunicación de certificados e informes de auditoría, podría conllevar la facturación de gastos adicionales considerables.

12.5 Cualquier información que se le proporcione al Cliente en aplicación de esta sección y que no esté disponible en el Sitio Web de OVHcloud será considerada como información confidencial de OVHcloud, según lo dispuesto en el Contrato. Antes de comunicar dicha información, OVHcloud podrá exigir al Cliente la celebración de un contrato de confidencialidad específico.

12.6 Con independencia de lo anterior, el Cliente está autorizado a responder a las solicitudes por parte de la autoridad de control pertinente, a condición de que la información facilitada se limite estrictamente a la solicitada por la autoridad de control. En tal caso, y salvo que la legislación aplicable lo prohíba específicamente, el Cliente deberá consultar previamente a OVHcloud la comunicación de cualquier información solicitada.

13. Contactar OVHcloud

Para cualquier pregunta relacionada con datos personales (incidente, condiciones de uso, etc.), el Cliente puede contactar a OVHcloud por uno de los siguientes medios:
(a) Creación de un ticket en su interfaz de gestión de cuenta,
(b) Uso del formulario de contacto provisto para este fin en el sitio web de OVHcloud,
(c) Al contactar a su Servicio de Soporte OVHcloud,
(d) Por correo postal a la dirección: OVH SAS, Oficial de Protección de Datos, 2 rue Kellermann, 59100 Roubaix (Francia).

STANDARD CONTRACTUAL CLAUSES

Transfers from processor to processor

PREAMBLE

OVH SAS is the (direct or indirect) parent company of the OVH European Affiliates.

OVH SAS and the OVH European Affiliates are selling services, including without limitation infrastructure as a service and cloud services (together the "**Services**").

As part of their activities and notably the execution of the Services, OVH SAS and the OVH European Affiliates are processing personal data subjected to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), notably personal data of their Clients.

Such personal data processing activities are performed by OVH SAS and the OVH European Affiliates either (a) as controller or (b) as a processor under their Clients' instructions.

OVH SAS and the OVH European Affiliates, at the express request of their Clients, may transfer the aforementioned processing activities to one or more data importers located in a country which is not considered by the European Commission as a third country that ensures an adequate level of protection according to article 45 of the GDPR. Such processing activities will be performed by the relevant data importer as a processor under instruction of the relevant data exporter. The performance of such processing activities implies a transfer of personal data to the data importer (including remote access from its country).

The data importer's country is not considered by the European Commission as a third country that ensures an adequate level of protection according to article 45 of the GDPR.

For the purposes of Articles 28 (7) and 46 (c) of the Regulation (EU) 2016/679,, the parties have agreed on the following Contractual Clauses adopted by Decision n°2021/914/EU dated 4 June 2021 of the European Commission, which integrates the clauses of Module 3 applicable to transfers from processor to processor (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

The following Clauses are only applicable to personal data processing activities performed by OVH SAS and the OVH European Affiliates as processor under their Clients' instructions entrusted to the relevant data importer as a processor.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the legal persons (hereinafter 'entities') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entities in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfers

The details of the transfers, and in particular the categories of personal data that are transferred and the purposes for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the

instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to

ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Parties for any damages it causes the other Parties by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause

16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations

under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data

to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) THE PARTIES AGREE THAT THOSE SHALL BE THE COURTS OF FRANCE.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

1. LIST OF PARTIES

Data exporter (processor)

France

OVH SAS Company incorporated under French Law whose registered office is located at 2 rue Kellermann 59100 Roubaix (France),

Austria

OVH Austria GmbH Company incorporated under Austrian Law whose registered office is located at Bureau 15722155, 1st, 2nd floor, Kohlmarkt 8-10, Vienna, 1010, Austria

Belgium

OVHCloud Belgium Company incorporated under Belgian Law whose registered office is located at 14 rue de Grand-Bigard, 1082 Berchem-Ste-Agathe, Belgium

OVHcloud DC Belgium SRL Company incorporated under Belgium Law whose registered office is located at 14 rue de Grand-Bigard, 1082 Berchem-Ste-Agathe, Belgium

Bulgaria

OVHcloud DC Bulgaria LLC. Company incorporated under Bulgarian Law whose registered office is located at 3 Moskovska str., Oborishte District, 1000 Sofia, Bulgaria

Czech Republic

OVHcloud DC CZ s.r.o Company incorporated under Czech Republic law whose registered office is located at Londýnská 254/7 120 00 Praha 2, Czech Republic

Denmark

OVHcloud DC Denmark ApS Company incorporated under Danish law whose registered office is located at NJORD Law Firm, Pilestræde 58, 6., 1112 København K, Denmark

Finland

OVHcloud DC Finland Oy Company incorporated under Finnish law whose registered office is located at Forvis Mazars Oy Bulevardi 21 00180 Helsinki, Finland

Germany

OVH GmbH Company incorporated under German law whose registered office is located at Christophstraße 19, 50670 Köln, Germany, **DCD Data Center Deutschland GmbH** Company incorporated under German law whose registered office is located at Oskar Jäger StraBe 173/K6 -50825 Köln, Germany

Gridscale GmbH Company incorporated under German law whose registered office is located at Oskar Jäger StraBe 173/K6 -50825 Köln, Germany

Italy

OVH SRL Company incorporated under Italian law whose registered office is located et Via Carlo Imbonati 18, CAP 20159 Milano

OVHcloud DC Italy S.R.L Company incorporated under Italian law whose registered office is located et Via Carlo Imbonati 18, CAP 20159 Milano, Italy

Ireland

OVH Hosting Limited Company incorporated under Irish law whose registered office is located at Block 3, Harcourt Centre, Harcourt Road, Dublin 2 D02 A339 Dublin 2, Ireland

OVHcloud DC Ireland Limited Company incorporated under Irish law whose registered office is located at Block 3, Harcourt Centre, Harcourt Road, Dublin 2 D02 A339 Dublin, Ireland

Luxembourg

OVHcloud DC Luxembourg SARL Company incorporated under Luxembourg law whose registered office is located at 5, rue Guillaume J. Kroll, L-1882 Luxembourg

Netherlands

OVH BV Company incorporated under Dutch law whose registered office is located at Hogehilweg 16, 1101 CD Amsterdam-Zuidoost, Netherlands

OVHcloud DC Netherlands B.V under Dutch law whose registered office is located at Hogehilweg 16, 1101 CD Amsterdam-Zuidoost, Netherlands

Norway

OVHcloud DC Norway Company incorporated under Norwegian law whose registered office is located at Fridtjof Nansens vei 19, 0369 Oslo, Norway

Poland

OVH Sp. Zo.o. Company incorporated under Polish law whose registered office is located at ul. Swobodna 1, 50-088 Wrocław , Poland

Data Center Ozarow Company incorporated under Polish law whose registered office is located at ul. Kazimierza Kamińskiego 6, 05-850 Ożarów Mazowiecki, Poland

Portugal

OVH Hosting Sistemas informaticos unipessoal Company incorporated under Portuguese law whose registered office is located at Praça de Alvalade, nº 7, 7º dtº 1700 036 Lisboa, Portugal

Romania

OVHCloud DC RO S.R.L Company incorporated under Polish law whose registered office is located at Bucuresti Sectorul 2, strada george constantinescu, nr. 4b si 2-4, camera 4a, bl. cladirea b, etaj 5, Romania

Spain

OVH Hispano Company incorporated under Spanish law whose registered office is located at C/ Alcalá 21, 5° planta, 28014 Madrid, Spain

Switzerland

OVHcloud DC Switzerland SA Company incorporated under Spanish law whose registered office is located at Mazars SA Rue de la Jeunesse 1 2800 Delémont, Switzerland

OVH SAS and OVH European Affiliates contact point for standard contractual clauses:

OVH - Data Protection Officer - 2 rue Kellerman 59100 Roubaix France

Activities relevant to the data transferred under these Clauses:

Computing, storage and/or any such other Services as described in the agreement concluded with the Clients.

Data importer (processor)

OVH Australia PTY Ltd, Company incorporated under Australian law whose registered office is located Level 12 - 90 Arthur Street, North Sydney NSW 2060, registered under company number 612612754. (Australia) Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	**Data Center Sydney PTY Ltd,** Company incorporated under Australian law whose registered office is located Level 12 - 90 Arthur Street, North Sydney NSW 2060 (Australia). Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
Hebergement OVH CANADA INC.	**OVH Serveurs INC.**

Company incorporated under Canada law whose registered office is located at 800-1801 Avenue McGill College, Montréal, QC, H3A 2N4 Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services** **OVH infrastructures Canada INC.** Company incorporated under Canada law whose registered office is located at 50 rue de l'Aluminerie Beauharnois, Québec, J6N 0C2 Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	Company incorporated under Canada law whose registered office is located at 50 rue de l'Aluminerie Beauharnois, Québec, J6N 0C2 Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
OVH Tech R&D Private Limited, Company incorporated under Indian law, whose registered office is located at Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India Contact point: Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such**	**Altimat Data Center India Private Limited,** Company incorporated under Indian law, whose registered office is located at H No. 215, A102 1st Floor A Wing, Narpoli, Golden Park, Rallway Stn Road, Anjur Phata, Bhiwandi, Thana, Maharashtra, India, 421302 Contact point: Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India

other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services	Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
Morocco OVH Hosting Company incorporated under Maroccan law, whose registered office is located at Espace Porte d'Anfa 3, rue Bab Mansour, Casablanca Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	**OVHcloud DC Morocco SARL** Company incorporated under Maroccan law, whose registered office is located at Espace Porte d'Anfa 3, rue Bab Mansour, Casablanca Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
OVHCloud Datacenter Mexico S. de R.L de C.V Company incorporated under Mexican law, whose registered office is located at Av. Paseo de la Reforma 295, Piso 10 Col. Cuauhtémoc, Del. Cuauhtémoc Ciudad de México, México Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	
New Zealand Company incorporated under New Zealand law, whose registered office is located at Level 35, Vero Centre, 48 Shortland Street, Auckland 1010 Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	
Sénégal OVH SARL Company incorporated under Senegalase law whose registered office is located at Avenue Abdoulaye Fadiga, immeuble Lahad Mbacké Dakar	

Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	
OVH Singapore PTE Ltd, Company incorporated under Singaporean law whose registered office is located at 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore). Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services** **Contact point for Singapore and Australia entities:** **OVH Singapore PTE Ltd,** 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore).	**Altimat Data Center Singapore PTE. Ltd,** Company incorporated under Singaporean law whose registered office is located at 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore) Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
Tunisie OVH SARL Company incorporated under Tunisian law whose registered office is located at Rue du Lac d'Annecy Passage du lac Malawi Les berges du lac 1053, Tunis Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	**OVH SARL** Company incorporated under Tunisian law whose registered office is located at Rue du Lac d'Annecy Passage du lac Malawi Les berges du lac 1053, Tunis Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
United Kingdom	**OVH LIMITED**

Data Center Erith LTD Company incorporated under UK law whose registered office is located at 30 Old Bailey, London EC4M 7AU Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	Data Center Erith LTD Company incorporated under UK law whose registered office is located at 30 Old Bailey, London EC4M 7AU Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**

2. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The categories of data subjects are determined and controlled by the Clients, at their sole discretion.

Categories of personal data transferred

Personal data used by the Clients within the Services including but not limited to any personal data stored by the Clients on, and/or computed by the Clients using, OVH SAS' and OVH European Affiliates' infrastructures. The categories of such personal data are determined and controlled by the Clients, at their sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The categories of such personal data are determined and controlled by the Client, at its sole discretion.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer is determined by the Clients, at their sole discretion.

Nature of the processing

The nature of processing activities carried out by the data importer on personal data may be computing, storage and/or any such other Services as provided in the agreement in force between OVH SAS or the OVH European Affiliates and the respective Client.

Purposes of the data transfer and further processing

Process the personal data to the extent necessary to provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The processing activities are performed for the duration provided in the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

When processors external to the OVH Group are involved in the processing of personal data carried out, this is mentioned in the terms and conditions applicable to the services concerned.

3. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority in accordance with Clause 13

- **France - Commission Nationale de l'Informatique et des Libertés - CNIL**

8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02. Tel. +33 1 53 73 22 22

- **Austrian Data Protection Authority**

Österreichische Datenschutzbehörde Barichgasse 40-42 1030 Wien Autriche**.** Tel +43 1 52 152-0

- **Belgium Gegevensbeschermingsautoriteit (APD-GBA)**

Rue de la Presse 35 / Drukpersstraat 35, 1000 Bruxelles / Brussel. Tel +32 2 274 48 00

- **Bulgaria Commission for Personal Data Protection**

2, Prof. Tsvetan Lazarov Blvd., Sofia 1592. Tel +359 2 915 3580

- **Czech Republic Office for Personal Data Protection**

Pplk. Sochora 27, 170 00 Praha 7. Tel +420 234 665 111

- **Denmark Danish Data Protection Agency (Datatilsynet)**

Carl Jacobsens Vej 35, 2500 Valby, Denmark- Tel +45 33 19 32 00

- **Finland Office of the Data Protection Ombudsman**

P.O. Box 800, FI-00531 Helsinki, Finland. Tel +358 29 56 66700

- **Germany - Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**

Husarenstraße 30 - 53117 Bonn. Tel. +49 228 997799 0

- **Ireland Data Protection Commission**

6 Pembroke Row, Dublin 2, D02 X 963, Irlande. Tel: +353 57 868 4800

- **Italy - Garante per la protezione dei dati personali**

Piazza Venezia, 1100187 Roma. Tel. +39 06 69677 1 • e-mail: garante@garanteprivacy.it

- **Luxembourg National Commission for Data Protection.**

15, Boulevard du Jazz, L-4370 Belvaux, Luxembourg. Tel +352 26 10 60 1

- **Netherlands - Autoriteit Persoonsgegevens**

Hoge Nieuwstraat 8 P.O. Box 93374 2509 AJ Den Haag/The Hague. Tel. +31 70 888 8500. E-mail: info@autoriteitpersoonsgegevens.nl

- **Norway Datatilsynet P.O.**

Box 458 Sentrum 0150 Oslo. Tel. +47 22 39 69 00

- **Poland - Urząd Ochrony Danych Osobowych (Personal Data Protection Office)**

ul. Stawki 2 00-193 Warsaw Tel. +48 22 531 03 00

- **Portugal - Comissão Nacional de Protecção de Dados - CNPD**

Av. D. Carlos I, 134, 1º 1200-651 Lisboa. Tel. +351 21 392 84 00. E-mail: geral@cnpd.pt

- **Romania National Supervisory Authority for Personal Data Processing (ANSPDCP)**

28-30 B-dul Magheru, Sector 1, 010336 Bucharest, Romania. Tel +40 318 059 211

- **Spain - Agencia de Protección de Datos**

C/Jorge Juan, 6 28001 Madrid .Tel. +34 91399 6200. E-mail: internacional@agpd.es

- **Suisse- Federal Data Protection and Information Commissioner (FDPIC)**

Feldeggweg1. 3003 Berne SUISSE. Tel +41 58 462 43 95

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The applicable security principles and rules are defined by the security team in partnership with OVHcloud top management. The security team, under the responsibility of the CISO, is itself composed of 4 teams:

The **security.tools** team in charge of developing the security tool used within OVHcloud. This team designs and operates the tools to support certain security measures deployed on all OVHcloud information systems. These tools include the management of the identities and accesses of employees and service providers, authentication mechanisms made available to clients, identification of vulnerabilities on systems and security monitoring. This team also assists other business teams in the design and deployment of architectures by ensuring security from the definition phase onwards.

The **security.operations** team is responsible for supporting teams in the implementation of good security practices within operations, the implementation of formal security management processes, the support in the integration of security tools and the alignment of security devices within OVHcloud. The security.ops team puts in place an internal control system, both organizational and technical on security and assists the product teams in the implementation of formal information security management systems and in their certification.

The **security.cert** team is responsible for monitoring threat sources, identifying attack tools and methods to anticipate them, and managing malicious security incidents. This team manages the OVHcloud CSIRT and exchanges with international expert communities to provide the best sources of information to anticipate attacks.

The **security.customer** team is in charge of adapting the products offered by OVHcloud to the specific needs of specific business sectors (healthcare, finance, etc.). The team values the expectations of these business sectors, and coordinates OVHcloud's response to contractual and standard compliance. It also provides level 3 support for customer questions about compliance and information security.

The security team is accompanied by the **physical security management teams** and the **privacy teams**. These three teams work together to ensure optimal effectiveness of actions on these subjects with strong adherence.

In addition, security referees are deployed within OVHcloud teams. These focal points enable the dissemination of good practices within teams, provide an identified point of contact for incident and crisis management, and enable the gathering of information from operations to the security team.

A security committee led by the CISO and the managers of the security team ensures communication with the Executive Committee (ComEx) of OVHcloud. This semi-annual committee presents the main threats under surveillance, the major risks, the monitoring metrics, the progress of the ongoing actions and the updated roadmap. This committee also ensures that the ISSP is aligned with OVHcloud's strategic and operational objectives.

Security compliance management

The ISMS aims to ensure that the security requirements of the various interested parties of OVHcloud

are taken into account. These requirements are of different kinds:

- legal or regulatory requirements
- contractual commitments
- good practices on which OVHcloud is committed explicitly

OVHcloud must identified and consolidate those requirements and implement the management system in support for the compliance to these requirements.

Documentation

OVHcloud must deploy a formal documented management system to :

- provide a comprehensive framework for policy rules, guideline, operational documentation, records and indicators
- ensure formalism and follow-up of activities implemented to reduce risks
- demonstrate compliance with applicable legal, regulatory or contractual requirements
- demonstrate compliance with the rules set out in the detailed security policies

Assets management

OVHcloud must deploy a formal approach for managing assets carrying security risks or in support for security management to ensure appropriate security controls over them:

- Maintain accurate inventories of those assets
- Define and maintain ownership for those assets
- Classification of those assets based on appropriate criteria to support security decision
- Definition of security rules adapted to their criticality

Security risks management

OVHcloud must deploy a risk management approach to structure operational decisions affecting security. This risk management approach is based on the principles of ISO/IEC 31000 and ISO/IEC 27005 standards. It is based on:

- In-depth knowledge of systems through asset cartography, asset classifications and valuations from a security perspective
- Ongoing analysis of feared events, vulnerabilities, and the threat environment
- uniform formalization of security risks to make them explicit to technical experts and decision-makers for reasonable and informed decision-making
- follow-up of decisions and action plans following the identification of a risk

The establishment of formal risk management enables the operational specificity of a project or product to be taken into account and the achievement of specific security objectives. Failure to comply with a ISSP rule results in an analysis of the risks resulting from the introduction of compensatory security measures to achieve at least an equivalent level of safety or acceptance of risk.

Privacy

The legislation applicable to the protection of personal data and our privacy policy constitute the framework for the processing of this data that OVHcloud applies. ISMS complements this

framework by consistently defining, implementing, and improving security arrangements that ensure the protection of hosted personal data.

This commitment is reflected in particular in:

- The implementation of a Personal Information Management System (PIMS) integrated with ISMS
- Setting up a joint management instance between the security and privacy teams
- Alignment of security and data usage policies
- Integrating security measures within ISMS into contractual commitments on personal information protection with customers
- The privacy team's participation in ISMS management
- Involvement of the security team in efforts to identify privacy risks
- Joint participation in resolving security incidents that impact personal information
- Joint definition of security objectives and measures to be implemented in the context of projects.

Customer Protection

OVH implements means of protection on the tools made available to these customers as well as on the communication channels between them and OVHcloud such as: :

- Customer interfaces through the use of identification factors ;
- Tools of detection and alerting when customer credentials are used for illegitimate purpose;
- Protection of customer infrastructures and services against external threats
- data related to customer managed by OVHcloud

Moreover, OVHcloud protects its communications with customers with adequate means according to the context like encrypted channels, collaborative tools with access and security controls or any other means defined with customers.

Customer trust

OVHcloud must provide the adequate transparency to customer in order the assist them in defining the right product for their needs. In particular, OVHcloud must provide information about :

- Physical location of the data and workloads hosting
- Physical location of the control plane and administrators
- Physical location of the support teams
- Applicable law for the service contract
- Supply chain and technical dependencies (Hardware, Software, Subcontractors)
- Reversibility capabilities information
- Certification and assurance mechanisms in place

Customer in cloud security

OVHcloud must produce a clear definition of responsibilities between OVHcloud and customer:

- Assets ownership
- Operations responsibility
- Security risk ownership
- Recommendation of security controls to implement by customer with OVHcloud included features and configuration
- Recommendation of security controls to implement by customer with optional features or external means when relevant

Security Ecosystem

OVHcloud must maintain close relationship with security communities to improve the quality of risk mitigation and accelerate response time to security threats. Security communities are covering but not limited to :

- Security experts, internally and externally
- Security team from hardware manufacturers
- Security team of software editors
- Open source groups
- Security software editors
- Security professional services providers

External technical reputation

OVHcloud must implement a set of processes to ensure the technical reputation of all systems exposed on public networks, since OVHcloud customers are relying on OVHcloud assets for their own information system. This covers:

- IP reputation to ensure that IP allocated to a customer infrastructure are usable for all legitimate purposes
- Abuse process to handle the dispute process when customer infrastructures are used for malicious activities
- Anti-fraud process to ensure all infrastructure usage is legitimate
- Anti-hack process to take down customer compromised infrastructures
- Spam, phishing, malware and dDoS detection and mitigation to protect the public from threats that might be hosted on OVHcloud infrastructure
- Protection and management of all assets under OVHcloud responsibility connected to public networks

Information system user

OVHcloud must protect information and systems by ensuring the information system is adequately operated:

- users are aware of the rules applicable to IS usage
- Company owned device management
- Employee owned device management
- Access to IS from external devices
- Collaborative tools
- Workstation security
- Mobile devices

Human resources

OVHcloud must integrate security topic into HR processes to ensure adapted resources are available to meet security objectives. This includes:

- security investments and human resources related to security priorities
- development of roadmaps of other OVHcloud teams to integrate security needs (investment and human resources)
- skills and training requirements for teams and inclusion in the training plan

- identifying gaps between needs and available resources for the adaptation of roadmaps and taking into account in risk management.

OVHcloud must educate employees on security as soon as they are integrated and throughout their presence in OVHcloud. This awareness is realized by:

- IT policy document to define the rules of usage of information system
- On boarding awareness session for all employees
- Formal threat presentation sessions targeting OVHcloud and security features in place
- Regular communications on good practices and risks
- Communications focused on a specific threat, related to current events or our detection activities
- Tests of the reflexes and the reaction capabilities of the collaborators
- Sharing information resources and feedback on cloud threats and vulnerabilities

OVHcloud must manage security in the complete employee life-cycle:

- Background check fitted to position criticality
- On boarding management including contractual commitment and awareness management
- Specific security training depending of position criticality
- Regular awareness session
- Disciplinary process for security violation
- Termination of contract management

Identity and access management

OVHcloud must maintain a strict policy of logical access rights management for employees :

- all employees use nominative user accounts to access any system
- generic and anonymous accounts is prohibited for any human access
- authorizations are issued and monitored by managers, following the principle of least privilege and the principle of gradually gaining trust
- to the greatest extent possible, all authorizations should be based on roles rather than unit rights
- a formal, fully auditable process is in place for account creation, modification, deletion and password change
- connection sessions systematically have an expiry period suited to each application
- user accounts are automatically deactivated if the password is not renewed after 90 days
- password complexity is mandatory based on best practices and recommendations from authorities:
    - users use automatic password generators rather than choosing their own passwords
    - Complexity rules are defined and communicated to all employees, and when possible technically enforced on systems
    - passwords must be renewed regularly, with a maximum of 90 days
- storing passwords in unencrypted files, on paper or in web browsers is prohibited

OVHcloud must maintain a strict policy of for managing administrator access rights for platforms :

- all administrator access to live systems is realized via a bastion host
- administrators connect to the bastion hosts via SSH, using individual and nominative pairs of public and private keys
- connection to the target system is realized either via a shared service account or via a nominative account and bastion hosts; using default accounts on systems and equipment is prohibited;
- dual-factor authentication is mandatory for remote administrator access and for any employees accessing sensitive areas of the system, with such access being fully traced

- administrators have an account exclusively devoted to administration tasks, in addition to their standard user account;
- authorizations are granted and monitored by managers, in accordance with the principle of least privilege
- SSH keys are protected by a password that meets the requirements of the password policy

Cryptography

- Use strong cryptography to secure data at rest and in transit and administration operations.
    - Manage cryptographic assets with automated process
    - Monitor certificates and keys to ensure all systems have valid certificates at all time

Physical security

OVHcloud physical security is based on zoning. Each area within OVHcloud premises is categorized in a zone type dependent from the area usage and the sensitivity of operations and assets hosted. At each zone type, according to it's sensitivity is defined security controls on:

- Environmental protection against fire, flood, weather conditions our any applicable environmental hazard related to premises location
    - Monitoring of any malicious or accidental events with automated (CCTV, sensors) or human (security watch)
    - Zone control, with a formal definition of all zones interfaces and gateway
    - Access control to ensure only authorized people access each zone for legitimate purpose

Supply Chain

OVHcloud's product teams rely mainly on other OVHcloud teams, but also on partners, subcontractors and suppliers to manage operations, and to compose products and services delivered to customers. The match between the outsourced activities and OVHcloud's security commitment must be managed:

- Identify dependencies between OVHcloud teams and subcontractors, suppliers and partners
    - Classification of criticality dependencies
    - Risk analysis and risk reduction where necessary
    - Service level cascade and security commitments
    - Integrating security into projects
    - Security insurance plan for subcontractors

Architecture

OVHcloud must ensure that cloud architecture is designed to be and stay secure taking into account the complexity of information system required to deliver the service, the factorization of information systems assets to optimize ressources and the management of several generations of technologies. We rely on several pillars to achieve this objective:

- Strong segregation of systems by criticality
- Mutualization of security primitives under the management of security team
- Harmonization of management of specific security assets and processes under common management rules
- Strong automation for security deployment

OVHcloud security team maintain a list of basic security architecture guidelines for systems. Architecture principles must be defined and documented for each type of infrastructure internally. OVHcloud uses several classification scheme for IT architecture depending of needs.

Exemples of classification:

- Tiers 0, Tiers 1, Tiers 2 for internal IS, depending of the internal usage
- Mutualized control plane
- Product dedicated control plane
- Customer infrastructure (Data plane)

Classification scheme must be used to define the set of security controls to apply according to the threat environment relevant to the classification characteristics.

Configuration and hardening

- Use OS patterns with system exposure minimization and baseline of security tools
- Use hardened kernels
- Follow best practices for configuration
- Deploy system as code with automated deployment tools
- Regularly review configurations for security

Administration

OVHcloud maintain those rules for administration activities:

- all administrator access to live systems is realized via a bastion host
- administrators connect to the bastion hosts via SSH, using individual and nominative pairs of public and private keys
- connection to the target system is realized either via a shared service account or via a nominative account and bastion hosts; using default accounts on systems and equipment is prohibited
- dual-factor authentication is mandatory for remote administrator access and for any employees accessing sensitive areas of the system, with such access being fully traced
- administrators have an account exclusively devoted to administration tasks, in addition to their standard user account
- authorizations are granted and monitored by managers, in accordance with the principle of least privilege and the principle of gaining trust
- SSH keys are protected by a password that meets the requirements of the password policy; access rights are reviewed on a regular basis, in collaboration with the departments concerned

Vulnerability and patch management

OVHcloud must ensure a systematic deployment of available security patches within a time frame defined by system based on its criticality. Vulnerabilities on systems must be identified and evaluated as soon as the associated patch is available. The application of the patch outside the predefined time limit must be justified on the basis of the level of risk associated with the corrected vulnerability or the existence of compensatory controls reducing the risk to an acceptable level.

- System owners are responsible of vulnerabilities management of their systems
- Assets shall be classified in terms of criticality
- Patch deployment is based on asset criticality and prioritization of patch deployment is based on risk level

- Vulnerability mitigation can be achieve without patch deployment, in that case, a complete analysis of the situation must be performed

OVHcloud must complete this process by a threat intelligence process and vulnerabilities monitoring to ensure all vulnerabilities that could put systems at risk are mitigated.

Monitoring and detection

OVHcloud must log all records necessary to understand any security events:

- logs are backed up and not limited to local storage
- logs are consulted and analyzed by a limited number of authorized personnel, in accordance with the authorization and access management policy
- tasks are divided up between the teams responsible for operating the monitoring infrastructure and the teams responsible for operating the service

The list of activities that are logged includes the following:

- logs of storage servers hosting customer data;
- logs of the machines managing the customer's infrastructure;
- logs of the machines monitoring the infrastructures;
- logs of the antivirus software installed on all equipped machines;
- integrity checks of logs and systems, where appropriate;
- tasks and events carried out by the customer on their infrastructure;
- network intrusion detection logs and alerts, if appropriate;
- logs of network equipment;
- logs of the infrastructure of the surveillance cameras;
- logs of administrator machines;
- logs of time servers;
- logs of badge readers;
- logs of bastion hosts.

OVHcloud implement tools and process to ensure:

- Fast detection of security events to minimize the occurrence of incidents and minimize impacts
- Adapted capabilities to investigate in post mortem

Change management

OVHcloud must maintain a formal change management principles including security :

- roles and responsibilities in security are clearly defined
- All changes are documented in tracking tool
- criteria for classification are set out in order to identify the security analysis to follow
- the risks associated with the changes are analyzed (if a risk is identified, the security manager and risk manager work together to validate the change)
- intrusion tests may be carried out (where applicable); the change is planned and scheduled with the customers (where applicable)
- the change is rolled out gradually (1/10/100/1000) and, if there is a risk, a rollback procedure is planned
- a retrospective review of the change is carried out

Each unit within OVHcloud implement its own change management procedure according to this principles.

Project management

OVHcloud integrates security within evolution and transformation projects. Compliance with ISSP and data protection is a general requirement for all OVHcloud activities. The security team assists OVHcloud project teams in the full lifecycle of all projects to ensure that the security means are adequate and properly implemented. This support consists of:

- Determine the security criticality of the data and processes involved in the project
    - Accompany project managers in the definition of technical and functional architecture
    - Support project teams in integration into the OVHcloud IS
    - Ensure compliance with the security base in the context of the project and the specific security measures to be put in place
    - Assist sponsors and project leaders in arbitrating specific measures against financial and operational constraints
    - Evaluate the security level of the project before production phase and after go-live
    - Identify residual risks and monitor them over time

Incident management

OVHcloud deploys a unified approach to security incident management by putting in place the organizational and technical means to:

- Detect and consolidate events that can impact the security of information systems and services
    - Correlate events that indicate a possible breach of information security and trigger incident handling as soon as possible
    - Mobilize experts and decision-makers in charge of resolving the incident
    - Support the incident with the following objectives
        - Reduce operational impacts
        - Preserve evidences to support possible judicialization or internal sanctions
        - Return to nominal situation
    - Inform interested parties in accordance with legal and contractual obligations
    - Identify root causes, update risk analysis, and define potential action plans to reduce the risk of a new occurrence

Network security

OVHcloud is managing a worldwide backbone to connect all infrastructures hosted in the datacenters and local networking to ensure the appropriate functioning and administration of the systems. The network security relies on:

- segmentation and segregation of network zones
- all networks equipment's are administered via a bastion host, applying the principle of least privilege
- access to the administration interfaces and administrator features for equipment is reserved to staff listed on control lists
- Network device inventory and automatized management
- Management of traffic and reaction to specific events
- Configuration of networks devices in terms of networking rules and access control
    - Administration of network based on automation. Configurations are deployed automatically, based on validated templates
    - Devices configuration are managed in a central configuration repository
    - A process is in place for ensuring changes are controlled

- the logs are collected, centralized and monitored on a permanent basis by the network operations team

Continuity

Continuity management relies on all mechanisms to ensure Availability, Rescue and Recovery.

Systems criticality must be defined to determine acceptable Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

System owners must implement controls to ensure the effectiveness ot continuity mechanisms.

Internal controls

First-level internal controls are deployed by the operational teams and the security team. These monitoring activities are mainly carried out in the form of:

- automated systems monitoring mechanisms
- operational checkpoints integrated into processes to ensure team coordination, risk accounting, and possible validations of risky activities. Where possible, these control points are integrated into the tools.
- ad hoc operational controls by security experts

Second-level internal control is carried out by the security teams to ensure the effectiveness of the first-level controls. These activities are formal.
The effectiveness of ISMS is also monitored in the context of steering activities.

Internal audits

OVHcloud relies on internal audit approaches to assess the effectiveness of internal control activities. These audits are performed by teams independent of audited operations and systems. Internal audit approaches include:

- Organizational and technical audit of the rules defined within ISSP
- Technical audit of architecture review, deployment, project
- Source code audit
- Intrusion tests

These steps are carried out by OVHcloud personnel or external contractors.

OVHcloud is implementing a public Bug Bounty program that will enable the permanent testing of our systems exposed on the internet.

These activities help identify vulnerabilities, non-conformities and opportunities for improvement and fuel the process of continuous improvement of security.

External audits

OVHcloud implements an external audit program on certified perimeters. We rely on:

- general security framework: ISO 27001, AICPA TSP (SOC)
- Cloud Provider-specific security framework: ISO 27017, CISPE, CSA CCM
- repositories dedicated to specific issues such as privacy: CISPE, ISO 27018, ISO 27701

- industry or geographical specific security framework: PCI DSS, HDS, PSEE, SecNumCloud, AGID, ENS, C5

For each framework, we determine the most appropriate certification or audit organization to strengthen our clients' confidence in our ability to meet the requirements that meet their expectations.

Audits by customers and authorities

OVHcloud allows its customers, under certain conditions, to perform security audits on systems.

Such audits may be:

- Technical, performed remotely (Intrusion Test, Vulnerability Scan) without OVHcloud teams intervention
- Organizational and technical in asynchronous way through questionnaires and written exchanges with OVHcloud
- On-site organizational and technical, including installation visits, interviews with operational staff, and access to documentation and configurations.

As with internal and external audits, these evaluations provide input to the security continuous improvement.

Continuous improvement

OVHcloud is implementing a continuous improvement of security and management processes. Opportunities for improvement are identified by:

- Internal control activities
- Internal and external audits
- Security Incident Analysis
- Identification of security risks
- Stakeholders involved in security management processes
- OVHcloud Security Interested Parties
- Analysis of root causes of non-conformities, vulnerabilities and incidents

These opportunities for improvement are evaluated before implementation and where appropriate prioritized and arbitrated. Consecutive action plans are formally followed in the project management tools used by teams

The processor adopts the same technical and organizational measures as the controller, listed above.