CONTRATO DE TRATAMENTO DE DADOS PESSOAIS

Última versão datada de 09.08.2023

O presente Contrato de Tratamento de Dados Pessoais ("**CTDP**"), parte integrante de qualquer acordo de prestação de serviços, referido doravante como "**Contrato**", é celebrado entre a OVH HOSTING Sistemas Informáticos Unipessoal, Lda. ("**OVHcloud**"), e o Cliente, e define os termos e condições aplicáveis aos serviços prestados pela OVHcloud (os "**Serviços**"). Este CTDP e outros contratos são complementares. Contudo, em caso de conflito, o CTDP prevalecerá.

Termos que comecem com letra maiúscula e que não estejam definidos neste CTDP terão o significado definido no Contrato. As expressões "Titular dos Dados", "Regras Vinculativas Aplicáveis às Empresas", "Responsável pelo Tratamento", "Dados Pessoais", "Violação de Dados Pessoais", "Tratamento", "Subcontratante", "Autoridade de Controlo" deverão ser interpretadas tal como definidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("**Regulamento Geral sobre Proteção de Dados**" ou "**RGPD**")

O objetivo deste CTDP é definir, nos termos do artigo 28.º do RGPD, as condições sob as quais a OVHcloud tem direito, como Subcontratante e como parte dos Serviços definidos no Contrato, para proceder ao tratamento por intermédio e sob instrução do Cliente, com exceção das atividades de tratamento de dados pessoais realizadas pela OVHcloud na qualidade de responsável pelo tratamento. As condições ao abrigo das quais a OVHcloud trata, como Responsável pelo Tratamento, Dados Pessoais relativos ao Cliente (incluindo os agentes do Cliente), encontram-se definidas na Política de Utilização de Dados da OVHcloud.

Para efeitos do presente CTDP, o Cliente pode atuar tanto como "**Responsável pelo Tratamento**" ou "Subcontratante relativamente aos Dados Pessoais. Se o Cliente estiver a atuar como Subcontratante em nome de um terceiro Responsável pelo Tratamento, as Partes concordam expressamente com as seguintes condições:

a. O Cliente deverá assegurar que (i) todas as autorizações necessárias para celebrar o presente CTDP, incluindo a indicação pelo Cliente da OVHcloud como subcontratante, foram obtidas junto do Responsável pelo Tratamento, (ii) um contrato, que esteja totalmente de acordo com os termos e condições do Contrato, incluindo este CTPD, foi celebrado com o Responsável pelo Tratamento de acordo com o referido artigo 28.º do RGPD, (iii) quaisquer instruções recebidas pela OVHcloud por parte do Cliente na execução do Contrato e deste CTPD estão totalmente de acordo com as instruções fornecidas pelo Responsável pelo Tratamento e (iv) toda a informação comunicada ou disponibilizada pela OVHcloud nos termos deste CTPD é adequadamente comunicada ao Responsável pelo Tratamento, conforme necessário;
b. a OVHcloud deve (i) tratar Dados Pessoais apenas sob as instruções do Cliente e (ii) não receber nenhuma instrução diretamente do Responsável pelo Tratamento, exceto nos casos em que o Cliente tenha desaparecido ou deixado de existir

juridicamente, sem que nenhuma entidade suceda nos direitos e obrigações do Cliente;

c. O Cliente, que é totalmente responsável perante a OVHcloud pela correta execução das obrigações do Responsável pelo Tratamento, conforme previsto no presente CTPD, deve indemnizar e afastar a responsabilidade da OVHcloud contra (i) qualquer falha do Responsável pelo Tratamento em cumprir a lei aplicável, e (ii) qualquer ação, reclamação ou queixa do Responsável pelo Tratamento relativa às disposições do Contrato (incluindo este CTPD) ou qualquer instrução recebida pela OVHcloud por parte do Cliente.

1. Âmbito

1.1 A OVHcloud está autorizada, como Subcontratante agindo sob instrução do Cliente, a tratar os Dados Pessoais do Responsável pelo Tratamento na medida necessária para prestar os Serviços.

1.2 A natureza das operações realizadas pela OVHcloud sobre Dados Pessoais pode ser de computação, armazenamento e / ou quaisquer outros Serviços, conforme descrito no Contrato.

1.3 O tipo de Dados Pessoais e as categorias de Titulares dos Dados são determinados e controlados pelo Cliente, a seu exclusivo critério.

1.4 As atividades de tratamento são realizadas pela OVHcloud pela duração prevista no Contrato.

2. Escolha de Serviços

2.1 O Cliente é o único responsável pela escolha dos Serviços. O Cliente deve assegurar que os Serviços escolhidos têm as caraterísticas e condições necessárias para cumprir as atividades e finalidades de tratamento do Responsável pelo Tratamento, bem como o tipo de Dados Pessoais a serem tratados nos Serviços, incluindo, mas não se limitando a, quando os Serviços são usados para tratar Dados Pessoais que estão sujeitos a regras ou padrões específicos (por exemplo, dados de saúde ou bancários em alguns países). O Cliente é informado de que a OVHcloud propõe determinados Serviços com medidas organizacionais e de segurança especificamente concebidas para o tratamento de dados de cuidados de saúde ou dados bancários.

2.2 Se o tratamento do Responsável pelo Tratamento puder resultar em alto risco para os direitos e a liberdade de pessoas físicas, o Cliente deverá selecionar cuidadosamente seus Serviços. Ao avaliar o risco, os seguintes critérios devem, nomeadamente, mas não apenas, ser tomados em consideração: avaliação ou pontuação dos Titulares de Dados; tomada de decisão automatizada com efeito legal ou similar significativo; monitorização sistemática dos Titulares de Dados; tratamento de dados sensíveis ou dados de natureza altamente pessoal; tratamento em larga escala; correspondência ou combinação de conjuntos de

dados; tratar dados relativos a Titulares de Dados vulneráveis; usando novas tecnologias inovadoras não reconhecidas pelo público, para o tratamento.

2.3 A OVHcloud disponibilizará informação ao Cliente, nas condições abaixo estabelecidas na secção "Auditoria", relativamente às medidas de segurança implementadas no âmbito dos Serviços, na medida necessária para avaliar a conformidade destas medidas com as atividades de tratamento do Responsável pelo Tratamento.

3. Cumprimento das Regras Aplicáveis

Cada Parte deve cumprir a legislação aplicável sobre proteção de dados (incluindo o Regulamento Geral sobre Proteção de Dados).

4. Obrigações da OVHcloud

4.1 A OVHcloud compromete-se a:

a. tratar os Dados Pessoais carregados, armazenados e utilizados pelo Cliente dentro dos Serviços apenas na medida em que sejam necessários e proporcionais para fornecer os Serviços, nos termos fixados no Contrato,
b. não aceder, nem utilizar os Dados Pessoais para qualquer outra finalidade que não seja a necessária para prestar os Serviços (especialmente em relação às finalidades de Gestão de Incidentes),
c. estabelecer as medidas técnicas e organizativas descritas no Contrato, para garantir a segurança dos Dados Pessoais na prestação do Serviço;
d. garantir que os funcionários da OVHcloud autorizados a tratar Dados Pessoais ao abrigo do Contrato estão sujeitos a uma obrigação de confidencialidade e recebem formação adequada sobre a proteção de Dados Pessoais,
e. informar o Cliente, se, na sua opinião e dadas as informações à sua disposição, uma instrução do Cliente infringir as disposições de proteção de dados do RGPD ou de outra disposição da União Europeia ou de um Estado-Membro da União Europeia.

4.2 No caso de pedidos recebidos de autoridades judiciais, administrativas ou outras para obter a comunicação de Dados Pessoais tratados pela OVHcloud ao abrigo do presente CTDP, a OVHcloud envida todos os esforços razoáveis para (i) analisar a competência da autoridade requerente e a validade do pedido, (ii) responder apenas a autoridades e pedidos que não sejam obviamente incompetentes e inválidos, (iii) limitar a comunicação aos dados pedidos pela autoridade e (iv) informar antecipadamente o Cliente (salvo quando proibido pela lei aplicável).

4.3 Se o pedido for feito por uma autoridade não europeia para obter a comunicação de dados pessoais tratados pela OVHcloud ao abrigo do presente CTDP em nome de um Cliente Europeu, a OVHcloud opõe-se ao pedido, nos seguintes casos:

(x) o pedido é feito em conformidade com um acordo internacional, como, por exemplo, um tratado de auxílio judiciário mútuo, em vigor entre o país requerente e a União Europeia ou o Estado-Membro onde os dados pessoais estão localizados ou o Estado-Membro da entidade OVHcloud para o qual o cliente registou a sua conta de cliente OVHcloud;
(y) os Dados Pessoais pedidos são armazenados num centro de dados localizado fora da União Europeia;
(z) o pedido é feito em conformidade com o artigo 49.º do RGPD, prossegue nomeadamente uma razão de interesse público importante reconhecida pela legislação da União Europeia ou dos Estados-Membros da União Europeia, ou é necessário para salvaguardar interesses vitais do titular dos dados ou de outras pessoas.

4.4 Mediante solicitação por escrito do Cliente, a OVHcloud fornecerá ao Cliente assistência razoável na realização de avaliações de impacto sobre a proteção de dados e consulta prévia à autoridade supervisora competente, se o Cliente estiver obrigado a fazê-lo, nos termos das regras de proteção de dados aplicáveis e, em cada caso, apenas na medida que tal assistência é necessária e se relaciona com o tratamento pela OVHcloud de Dados Pessoais deste CTPD. Essa assistência consistirá em fornecer transparência sobre as medidas de segurança implementadas pela OVHcloud na prestação dos seus Serviços.

4.5 A OVHcloud compromete-se a implementar as seguintes medidas técnicas e organizativas:

a. Medidas de segurança física destinadas a impedir o acesso de pessoas não autorizadas à infraestrutura onde estão armazenados os dados do Cliente;
b. verificações de identidade e de acesso utilizando um sistema de autenticação, bem como uma política de palavras-passe,
c. Um sistema de gestão do acesso que limite o acesso às instalações às pessoas que delas necessitem, no exercício das suas funções e no âmbito das suas responsabilidades;
d. pessoal de segurança responsável pelo controlo da segurança física das instalações da OVHcloud;
e. um sistema que física e logicamente isola os Clientes uns dos outros,
f. processos de autenticação de utilizadores e administradores, bem como medidas para proteger o acesso a funções de administração,
g. um sistema de gerenciamento de acesso para operações de suporte e manutenção que opera com base nos princípios dos “privilégios mínimos” (*principle of least privilege)* e necessidade de conhecimento (*need to know*), e
h. processos e medidas para rastrear ações executadas em seu sistema de informação.

4.6 Estas medidas técnicas e organizativas estão detalhadamente descritas na página da OVHcloud.

5. Violação de dados pessoais

5.1 Se a OVHcloud tomar conhecimento de um incidente que afete os Dados Pessoais do Responsável pelo Tratamento (como acesso não autorizado, perda, divulgação ou alteração de dados), a OVHcloud notificará o Cliente sem demora injustificada.

5.2 A notificação deve (i) descrever a natureza do incidente, (ii) descrever as consequências prováveis do incidente, (iii) descrever as medidas tomadas ou propostas pela OVHcloud em resposta ao incidente e (iv) fornecer o ponto de contacto da OVHcloud .

6. Localização e transferência de Dados Pessoais

6.1 Nos casos em que um Serviço permite ao Cliente armazenar Conteúdo e, nomeadamente, Dados Pessoais, a(s) localização(ões) ou área geográfica do(s) Centros(s) de Dados disponível(eis) é(são) especificada(s) no site da OVH. Se estiverem disponíveis vários locais ou áreas geográficas, o Cliente deverá selecionar o escolhido ao enviar o seu Pedido. Sujeito a qualquer disposição em contrária prevista nos Termos e Condições Especiais aplicáveis, a OVH não modificará, sem o consentimento prévio do Cliente, a localização ou a área geográfica escolhida ao enviar o seu Pedido.

6.2 Sujeito à disposição de localização dos Centros de Dados acima referida, a OVH e os Subcontratantes autorizados, de acordo com a secção 7 abaixo, podem tratar remotamente o Conteúdo do Cliente, desde que tais operações de tratamento ocorram na medida do necessário para a realização dos Serviços e, em particular, estejam relacionados com questões de segurança e manutenção do serviço.

6.3 Relativamente à utilização de Serviços localizados em Centros de Dados não europeus, (a) os Centros de Dados podem estar localizados em países que estão sujeitos a uma decisão de adequação da Comissão Europeia nos termos do artigo 45.º do RGPD ("Decisão de Adequação") e/ou (b) o Conteúdo do Cliente pode, secções 6.2 e 7 deste CTDP, ser tratado por esses países não sujeitos a uma Decisão de Adequação.

6.4 No caso do Cliente utilizar os Serviços referidos no parágrafo acima para efeitos de processamento de Dados Pessoais sujeitos à RGPD, o Cliente será considerado como Controlador, OVHcloud como seu Subcontratante e as subsidiárias de OVHcloud como Subcontratante subsequentes. Ao transferir dados pessoais para as suas filiais localizadas em Estados que não beneficiam de uma Decisão de Adequação, OVHcloud é considerado como Exportador de Dados e as suas filiais como Importador de Dados na aceção da RGPD. Neste contexto, OVHcloud e as suas filiais celebraram cláusulas contratuais-tipo adoptadas pela Comissão Europeia na sua decisão de aplicação (UE) 2021/914 de 4 de Junho de 2021 (doravante "Cláusulas Contratuais-tipo"), em anexo o presente DPA e destinadas a serem aplicadas a tais transferências.

6.5 Com respeito aos Serviços localizados em centros de dados situados dentro da União Europeia, se os Termos de Serviço aplicáveis estabelecerem que o processamento de Dados Pessoais sujeitos a este DPA é suscetível de ser efetuado a partir de um ou mais países que não beneficiam de uma Decisão de Adequação, as Cláusulas Contratuais Padrão acima mencionadas aplicar-se-ão.

6. 6. o Cliente continuará responsável por (a) avaliar a eficácia das Cláusulas Contratuais-tipo em anexo, incluindo as correspondentes medidas técnicas e organizacionais, em particular no que respeita às categorias de dados pessoais que o Cliente pretende tratar no contexto dos Serviços em questão, e do sistema jurídico e práticas do país ou países de

destino, ao fim de determinar se existem elementos suscetíveis de comprometer a eficácia das Cláusulas Contratuais-tipo, e (b) se se verificar que a eficácia das referidas Cláusulas Contratuais-tipo pode ser comprometida, aplicar, em conformidade com as recomendações do Comité Europeu de Proteção de Dados, medidas adicionais suscetíveis de assegurar um nível de proteção equivalente ao garantido no seio da União Europeia. OVHcloud compromete-se a assistir o Cliente na avaliação acima referida, comunicando-lhe, a seu pedido, qualquer informação útil em sua posse. Além disso, o Cliente permanece responsável pelo cumprimento de qualquer formalidade e/ou obtenção de qualquer autorização ou consentimento que possa ser necessário para permitir a transferência de dados pessoais para países que não beneficiam de uma Decisão de Adequação.

6.7 Quaisquer Cláusulas Contratuais-Tipo aplicáveis devem ser complementadas pelas outras Condições de Serviços aplicáveis (incluindo este CTDP) que se aplicam *mutatis mutandis* ao(s) Importador(es) de Dados e Exportador(es) de Dados, desde que não entrem em conflito com as Cláusulas Contratuais-Tipo. Em caso de conflito, prevalecerão as Cláusulas Contratuais-Tipo.

7. Contratação de um subcontratante para o tratamento

7.1 Sujeito às disposições da secção “Localização e transferência de dados pessoais” acima, a OVHcloud está autorizada a subcontratar para assistência na prestação dos Serviços. Como parte de tal assistência, os subcontratados podem participar das atividades de processamento de dados realizadas pela OVHcloud sob as instruções do Cliente.

7.2 A lista de subcontratantes que estão autorizados a participar das atividades de tratamento realizadas pela OVHcloud sob as instruções do Cliente ("Subcontratantes”), incluindo os Serviços em questão e o local a partir do qual eles podem processar os Dados Pessoais do Cliente de acordo com este Contrato, é fornecido (a) no site da OVHcloud ou, (b) quando um Subcontratante participa apenas num Serviço específico, nos Termos e Condições Específicos aplicáveis.

7.3 Se a OVHcloud decidir alterar um Subcontratante ou adicionar um novo Subcontratante (“**Alteração do Subcontratante**”), a OVHcloud notificará o Cliente no seu painel de controlo ou por email (para a morada de email registada na Conta do Cliente) (a) com trinta (30) dias de antecedência se o Subcontratante for uma Afiliado da OVHcloud localizado na União Europeia ou em um país sujeito a uma Decisão de Adequação ou (b) noventa (90) dias de antecedência em qualquer outro caso. O Cliente tem o direito de se opor a uma Alteração do Subcontratante, nos termos do RGPD. A objeção deve ser notificada à OVHcloud dentro de quinze (15) dias após o aviso de Alteração do Subcontratante por parte da OVHcloud ao Cliente e especificando o motivo da objeção. Essa objeção deve ser notificada pelo Cliente através do seu Interface de Gerenciamento, usando a categoria “Solicitação de Proteção de Dados” ou por escrito ao Encarregado de Proteção de Dados, OVHcloud SAS, 2 rue Kellermann 59100 Roubaix (França). A OVHcloud não deve, em caso algum, ser obrigada a renunciar a uma alteração de Subcontratante. Se, após a objeção de um Cliente, a OVHcloud não renunciar à alteração do Subcontratante, o Cliente tem o direito de encerrar os Serviços afetados.

7.4 A OVHcloud deverá assegurar que o Subcontratante é, no mínimo, capaz de cumprir as obrigações assumidas pela OVHcloud no presente CTPD relativamente ao tratamento de Dados Pessoais realizados pelo Subcontratante. Para o efeito, a OVHcloud deve celebrar um contrato com o Subcontratante. A OVHcloud permanecerá totalmente responsável perante o Cliente pelo desempenho de qualquer obrigação que o Subcontratante não cumpra.

7.5 A OVHcloud está pelo presente autorizada a contratar fornecedores terceiros (como fornecedores de energia, provedores de rede, gestores de pontos de interligação de rede ou instalações de centro de dados, fornecedores de material e software, transportadores, fornecedores técnicos, empresas de segurança), independentemente de onde se encontrem localizadas, sem ter de informar o Cliente ou obter sua aprovação prévia, desde que tais provedores de terceiros não procedam ao tratamento de Dados Pessoais do Cliente.

8. Obrigações do Cliente

8.1 Para o tratamento de Dados Pessoais, conforme previsto no Contrato, o Cliente deverá fornecer à OVHcloud por escrito (a) toda as instruções relevantes e (b) qualquer informação necessária para a criação dos registos do Subcontratante das atividades de tratamento. O Cliente é o único responsável por tais informações de tratamento e instruções comunicadas à OVHcloud.

8.2 O Cliente é responsável por garantir que:

a. o tratamento dos Dados Pessoais em execução do Serviço tem uma base legal apropriada (por exemplo, consentimento do Titular dos Dados, consentimento do Responsável pelo Tratamento, interesses legítimos, autorização da autoridade competente relevante, etc.),
b. são implementados todos os procedimentos e formalidades exigidos (como seja a avaliação de impacto sobre proteção de dados, solicitação de notificação e autorização à autoridade competente ou outro órgão competente, quando necessário),
c. os Titulares dos Dados são informados sobre o tratamento dos respetivos Dados Pessoais de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, conforme previsto no RGPD,
d. os Titulares dos Dados são informados e devem ter a todo o tempo a possibilidade de exercer facilmente os seus direitos conforme previsto no RGPD diretamente ao Responsável pelo Tratamento.

8.3 O Cliente é responsável pela implementação de medidas técnicas e organizativas no domínio da segurança dos recursos, sistemas, aplicações e operações que não estejam no âmbito de responsabilidade da OVHcloud, conforme definido no Contrato (nomeadamente, qualquer sistema e software implementado e executado pelo Cliente ou pelos Utilizadores no âmbito dos Serviços).

9. Direitos do titular dos dados

9.1 O Responsável pelo Tratamento é totalmente responsável por informar os Titulares dos Dados sobre os seus direitos, e por respeitar esses direitos, incluindo os direitos de acesso, retificação, exclusão, limitação, portabilidade ou apagamento.

9.2 A OVHcloud fornecerá cooperação e assistência razoáveis, conforme seja razoavelmente exigido para o propósito de responder aos pedidos dos Titulares dos Dados. A cooperação e a assistência razoáveis podem consistir em (a) comunicar ao Cliente qualquer solicitação recebida diretamente do Titular dos Dados e (b) permitir que o Responsável pelo Tratamento projete e implemente as medidas técnicas e organizativas necessárias para responder às solicitações dos Titulares dos Dados. O Responsável pelo Tratamento será o único responsável por responder a tais solicitações.

9.3 O Cliente reconhece e concorda que no caso de tal cooperação e assistência exigir recursos significativos por parte do Subcontratante, este esforço será exigível mediante aviso prévio e acordado com o Cliente.

10. Apagamento e devolução dos Dados Pessoais

10.1 Após o término de um Serviço (nomeadamente, em caso de rescisão ou não renovação), a OVHcloud compromete-se a apagar, nas condições previstas no Contrato, todo o Conteúdo (incluindo informação, dados, ficheiros, sistemas, aplicações, sítios da Internet e outros itens) que seja reproduzido, armazenado, hospedado ou de outra forma utilizado pelo Cliente no âmbito dos Serviços, a menos que um pedido emitido por uma autoridade legal ou judicial competente, ou a lei aplicável na União Europeia ou de um Estado Membro da União Europeia, exija o contrário.

10.2 O Cliente é o único responsável por assegurar que as operações necessárias (como *backup*, transferência para uma solução de terceiros, Instantâneos, etc.) para a preservação dos Dados Pessoais sejam realizadas, especialmente, antes do término ou expiração dos Serviços, e antes prosseguir com quaisquer operações de apagamento, atualizações ou reinstalação dos Serviços.

10.3 A este respeito, o Cliente é informado de que a rescisão e termo de um Serviço por qualquer motivo (incluindo, mas não limitado, à não renovação), bem como certas operações para atualizar ou reinstalar os Serviços, podem resultar automaticamente no apagamento irreversível de todo o Conteúdo (incluindo informações, dados, arquivos, sistemas, aplicativos, sítios da Internet e outros itens) que é reproduzido, armazenado, hospedado ou de outra forma utilizado pelo Cliente dentro do âmbito dos Serviços, incluindo qualquer potencial *backup*.

11. Responsabilidade

11.1 A OVHcloud só pode ser responsabilizada por danos causados no tratamento para os quais (i) não tenha cumprido as obrigações do RGPD especificamente relacionadas com tratamento de dados pelos Subcontratantes ou (ii) tenha agido de forma contrária às

instruções escritas lícitas do Cliente. Nesses casos, a disposição de responsabilidade do Contrato será aplicada.

11.2 Caso a OVHcloud e o Cliente estejam envolvidos num tratamento ao abrigo deste Contrato que tenha causado danos ao Titular dos Dados, o Cliente deve em primeiro lugar assumir a indemnização total (ou qualquer outra compensação) que seja devida ao Titular dos Dados e, posteriormente , reclamar à OVHcloud a parte da indemnização do Titular dos Dados correspondente à parcela da responsabilidade da OVHcloud pelos danos, desde que não seja aplicável nenhuma limitação de responsabilidade prevista no Contrato.

12. Auditoria

12.1 A OVHcloud disponibilizará ao Cliente toda a informação necessária para (a) demonstrar o cumprimento dos requisitos do RGPD e (b) permitir a realização de auditorias. Esta informação está disponível na documentação-tipo no site da OVHcloud. Podem ser comunicadas informações adicionais ao Cliente, mediante pedido ao Suporte da OVHcloud.

12.2 Se um Serviço for certificado, estiver em conformidade com um código de conduta ou estiver sujeito a procedimentos de auditoria específicos, a OVHcloud disponibiliza os certificados correspondentes e os relatórios de auditoria ao Cliente mediante pedido por escrito.

12.3 Se a informação, relatório e certificado acima mencionados se revelarem insuficientes para permitir ao Cliente demonstrar que cumpre as obrigações estabelecidas pelo RGPD, a OVHcloud e o Cliente reunir-se-ão para acordar as condições operacionais, de segurança e financeiras de uma inspeção técnica no local. Em todas as circunstâncias, as condições desta inspeção não devem afetar a segurança de outros Clientes da OVHcloud.

12.4 A referida inspeção no local, bem como a comunicação de certificados e relatórios de auditoria, pode resultar numa faturação adicional razoável.

12.5 Qualquer informação que seja comunicada ao Cliente nos termos desta secção e que não esteja disponível no sítio da Internet da OVHcloud, será considerada como informação confidencial da OVHcloud ao abrigo do Contrato. Antes de comunicar essa informação, poderá ser exigido ao Cliente que celebre um acordo específico de confidencialidade.

12.6 Não obstante o acima exposto, o Cliente está autorizado a responder às solicitações da autoridade supervisora competente desde que qualquer divulgação de informações seja estritamente limitada ao que é solicitado pela referida autoridade supervisora. Nesse caso, e a menos que seja proibido pela lei aplicável, o Cliente deve primeiro consultar a OVHcloud relativamente a qualquer divulgação requerida.

13. Contacte a OVHcloud

Para qualquer questão relacionada com os seus dados pessoais (incidentes, condições de utilização, etc.), o Clientes pode contactar a OVHcloud através dos seguintes canais de comunicação:

a. Criação de um *ticket* através do Interface de Gerenciamento da Conta de Cliente;

b. Utilização do formulário de contacto disponível para o efeito na página web da OVHcloud;

c. Através do contacto do Serviço de Suporte da OVHcloud;

d. Por correio para a seguinte morada; OVH SAS, Data Protection Officer, 2 rue Kellermann, 59100 Roubaix, França.

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

A. LIST OF PARTIES

Data exporter (processor)

OVH SAS

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

OVH Hispano

Company incorporated under Spanish law whose registered office is located et C/ Alcalá 21, 5° planta, 28014 Madrid (Spain),

OVH SRL

Company incorporated under Italian law whose registered office is located et Via Carlo Imbonati 18, CAP 20159 Milano (Italy),

OVH GmbH

Company incorporated under German law whose registered office is located at Christophstraße 19, 50670 Köln (Germany),

OVH Hosting Limited

Company incorporated under Irish law whose registered office is located at 38/39 Fitzwilliam Sqaure West Dublin 2 D02 NX53 (Ireland),

OVH Sp. Zo.o.

Company incorporated under Polish law whose registered office is located at ul. Swobodna 1, 50-088 Wrocław (Poland),

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),

OVH BV

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

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 Singapore PTE Ltd, Company incorporated under Singaporean law whose registered office is located 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**	**Altimat Data Center Singapore PTE. Ltd,** Company incorporated under Singaporean law whose registered office is located 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**
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**
Contact point for Singapore and Australia entities: **OVH Singapore PTE Ltd,** 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore).	
OVH Tech R&D Private Limited, Company incorporated under Indian law, whose registered office is located at Salapuria Symbiosis,	**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

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 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**	Road, Anjur Phata, Bhiwandi, Thana, Maharashtra, India, 421302 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 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**

B. 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.

C. 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

Spain - Agencia de Protección de Datos

C/Jorge Juan, 6 28001 Madrid

Tel. +34 91399 6200 • e-mail: internacional@agpd.es

Portugal - Comissão Nacional de Protecção de Dados - CNPD

R. de São. Bento, 148-3° 1200-821 Lisboa

Tel. +351 21 392 84 00 • e-mail: geral@cnpd.pt

Italy - Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121 00186 Roma

Tel. +39 06 69677 1 • e-mail: garante@garanteprivacy.it

Germany - Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30 - 53117 Bonn

Tel. +49 228 997799 0 • e-mail: poststelle@bfdi.bund.de

Netherlands - Autoriteit Persoonsgegevens

Prins Clauslaan 60 P.O. Box 93374 2509 AJ Den Haag/The Hague

Tel. +31 70 888 8500 • e-mail: info@autoriteitpersoonsgegevens.nl

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.