

TeamViewer

Data Processing Agreement (DPA)

ENGLISH

PORTUGUÊS

1 Applicability

For the data processing activities described in [Annex 1](#) of this agreement, where Customer acts as data controller and TeamViewer acts as the Customer's processor, the parties agree to the following provisions on the commissioned processing of personal data, which shall supplement the [TeamViewer End User License Agreement \(EULA\)](#) (Data Processing Agreement, **(DPA)**) until further notice.

The DPA does not apply if the Customer is a natural person using the Software or the Services in the course of a purely personal or family activity (cf. Art. 2(2)(c) EU General Data Protection Regulation (EU 2016/679), **(GDPR)**).

The provisions of this DPA and the EULA concluded at the same time complement each other and exist side by side. In the event of any contradictions in the area of data protection, the DPA shall take precedence over the provisions of the EULA.

For Customer's convenience, TeamViewer provides an overview of how it collects and processes personal data in connection with the use of TeamViewer Software and Services in its [Data Protection Information Sheet](#) for TeamViewer Customers, as amended from time to time.

2 Rights and obligations of TeamViewer

2.1 Applicable laws

The obligations of TeamViewer shall arise from this DPA and the applicable data protection laws. The applicable laws shall in particular include the German Federal Data Protection Act (*Bundesdatenschutzgesetz (BDSG)*) and the GDPR.

1 Aplicabilidade

Para as atividades de processamento de dados descritas em [Anexo 1](#) Neste acordo, em que o Cliente atua como controlador de dados e a TeamViewer atua como processadora de dados do Cliente, as partes concordam com as seguintes disposições sobre o processamento terceirizado de dados pessoais, que complementarão o presente acordo. [Contrato de Licença de Usuário Final do TeamViewer \(EULA\)](#) (Adendo de Processamento de Dados (ADP)) (**Adendo de Processamento de Dados (ADP)**) Até novo aviso.

A Adendo de Processamento de Dados (ADP) não se aplica se o Cliente for uma pessoa singular que utiliza o Software ou os Serviços no âmbito de uma atividade puramente pessoal ou familiar (cf. Art. 2(2)(c) Regulamento Geral de Proteção de Dados da UE (UE 2016/679), **(RGPD)**).

As disposições deste Adendo de Processamento de Dados (ADP) e do EULA, celebrados simultaneamente, Adendo de Processamento de Dados (ADP) Sobre as disposições do EULA.

Para maior conveniência do cliente, a TeamViewer fornece uma visão geral de como coleta e processa dados pessoais conexão ao uso do software e dos serviços da TeamViewer em sua Política de Privacidade. [Ficha de Informações sobre Proteção de Dados](#) Para clientes TeamViewer, conforme alterado periodicamente.

2 Direitos e obrigações do TeamViewer

2.1 Leis aplicáveis

As obrigações da TeamViewer decorrem deste Adendo de Processamento de Dados (ADP) e das leis de proteção de dados aplicáveis. As leis aplicáveis incluem, em particular, a Lei Federal Alemã de Proteção de Dados (*Bundesdatenschutzgesetz (BDSG)*) e o GDPR.

2.2 Processing on instructions only

To the extent this DPA is applicable, TeamViewer shall only process personal data within the scope of this DPA and on documented instructions of the Customer, which are mutually agreed upon by the parties in the EULA and especially defined by the Product functionality, unless TeamViewer is required to do so by European Union or member state law to which TeamViewer is subject; in such a case TeamViewer shall inform the Customer of that legal requirement before processing, unless the respective law prohibits such information on important grounds of public interest. The Customer can give additional written instructions as far as this is necessary to comply with the applicable data protection law. The documentation on issued instructions shall be kept by the Customer for the term of the DPA.

2.3 Obligation of confidentiality

TeamViewer shall ensure that the persons authorized to process the personal data are committed to confidentiality or under an appropriate statutory obligation of confidentiality.

2.4 Technical and Organizational Measures

TeamViewer has implemented and maintains reasonable and appropriate technical and organization measures regarding the protection of personal data in accordance with Art. 32 GDPR (**TOMs**). The TOMs are described in detail in the documentation of the TOMs, which is attached to this DPA as [Annex 2](#). Further information on TeamViewer's security can be found in [TeamViewer's Trust Center](#).

The TOMs take into account the state of art, the implementation costs, and the nature, scope, context and purposes of processing personal data to ensure a level of security appropriate to the risk to the rights and freedoms of the natural persons affected by the processing. To this end, the protection objectives of Art. 32 (1) GDPR, such as confidentiality, integrity and availability of systems and services and their resilience in terms of the nature, scope, as well as context of the processing shall be addressed in such a way that the risks are mitigated continuously by appropriate TOMs.

2.2 Processamento somente sob instruções

Na medida em que este Adendo de Processamento de Dados (ADP) for aplicável, a TeamViewer processará dados pessoais apenas no âmbito deste Adendo de Processamento de Dados (ADP) e mediante instruções documentadas do Cliente, mutuamente acordadas pelas partes no EULA e especificamente definidas pela funcionalidade do Produto, a menos que a TeamViewer seja obrigada a fazê-lo por lei da União Europeia ou de um Estado-Membro a que esteja sujeita; nesse caso, a TeamViewer informará o Cliente sobre essa exigência legal antes do processamento, a menos que a respectiva lei proíba tal informação por motivos importantes de Público. O Cliente pode fornecer instruções adicionais por escrito, sempre que necessário para cumprir a legislação de proteção de dados aplicável. Documentação relativa às instruções emitidas deverá ser mantida pelo Cliente durante a vigência do Adendo de Processamento de Dados (ADP).

2.3 Obrigação de confidencialidade

A TeamViewer garantirá que as pessoas autorizadas a processar os dados pessoais estejam comprometidas com a confidencialidade ou sujeitas a uma obrigação legal apropriada de confidencialidade.

2.4 Medidas técnicas e organizacionais

A TeamViewer implementou e mantém medidas técnicas e empresa razoáveis e adequadas em relação à proteção de dados pessoais em conformidade com o Art. 32 do RGPD. (**TOMs**). Os TOMs são descritos detalhadamente na documentação dos TOMs, que está anexada a este Adendo de Processamento de Dados (ADP) como [Anexo 2](#). Mais informações sobre a segurança do TeamViewer podem ser encontradas em [Central de Confiança do TeamViewer](#).

As medidas de otimização de tratamento (TOMs) levam em consideração o estado da arte, os custos de implementação e a natureza, Âmbito, o contexto e as finalidades do tratamento de dados pessoais para garantir um nível de segurança adequado ao risco para os direitos e liberdades das pessoas singulares afetadas pelo tratamento. Para tanto, os objetivos de proteção do 32.º, n.º 1, do RGPD, como a confidencialidade, a integridade e a disponibilidade dos sistemas e serviços e a sua resiliência em termos da natureza, do âmbito e do contexto do tratamento, devem ser abordados de forma a que os riscos sejam mitigados

The procedures for the regular review, assessment, and evaluation of the effectiveness of the then-current TOMs is further described in [Annex 2](#). The TOMs are subject to technical progress and further development. TeamViewer may review and update the TOMs from time to time without notification of the Customer, provided that any such update will not degrade the security of the personal data and of the Software and Services of TeamViewer.

2.5 Assistance with requests

TeamViewer shall, taking into account the nature of the processing, assist the Customer as far as this is possible by appropriate technical and organizational measures in the fulfillment of requests to exercise the rights of affected data subjects as referred in Chapter III of the GDPR. Should a data subject contact TeamViewer directly to exercise the data subject's rights regarding the data processed on behalf of the Customer (as far as identifiable), TeamViewer shall immediately forward such request to the Customer. Upon request, the Customer shall remunerate TeamViewer with an appropriate compensation for the effort resulting from such assistance, if and as far as permitted by applicable data protection laws.

2.6 Assistance with compliance with Art. 32 - 36 GDPR

Taking into account the type of processing and the information available to TeamViewer, TeamViewer shall support the Customer with appropriate technical and organizational measures to comply with the obligations mentioned in Art. 32-36 GDPR, especially with regard to the security of the processing, the notification of personal data breach, the data protection impact assessment as well as the consultation with supervisory authorities. Upon request, the Customer shall compensate TeamViewer an appropriate compensation for the effort resulting from such assistance, if and as far as permitted by applicable data protection laws.

2.7 Records of processing activities

TeamViewer will provide the Customer with the information necessary to maintain the records of processing activities.

continuamente por TOMs adequadas.

Os procedimentos para a revisão, avaliação e análise regulares da eficácia das TOMs vigentes são descritos em detalhes em [Anexo 2](#). Os Termos de Serviço estão sujeitos a progresso técnico e desenvolvimento contínuo. A Poderá revisar e atualizar os Termos de Serviço periodicamente, sem notificação ao Cliente, desde que tal atualização não comprometa a segurança dos dados pessoais, do Software e dos Serviços da TeamViewer.

2.5 Auxílio com solicitações

Considerando a natureza do processamento, a TeamViewer auxiliará o Cliente, na medida do possível, por meio de medidas técnicas e organizacionais. No atendimento às solicitações de exercício dos direitos dos titulares dos dados afetados, conforme mencionado no Capítulo III do RGD. Caso um titular dos dados entre em contato diretamente com a TeamViewer para exercer seus direitos em relação aos dados processados em nome do Cliente (na medida em que forem identificáveis), a TeamViewer encaminhará imediatamente tal solicitação ao Cliente. Solicitação, o Cliente remunerará a TeamViewer com uma compensação adequada pelo esforço decorrente de tal assistência, se e na medida em que for permitido pelas leis de proteção de dados aplicáveis.

2.6 Assistência no conformidade dos 32 a 36 do RGD.

Considerando o tipo de processamento e as informações disponíveis para a TeamViewer, esta deverá apoiar o Cliente com medidas técnicas e organizacionais adequadas para o cumprimento das obrigações mencionadas nos 32 a 36 do RGD, especialmente no que diz respeito à segurança do processamento, à notificação de violação de dados pessoais, à avaliação de impacto sobre a proteção de dados, bem como à consulta às autoridades de supervisão. Solicitação, o Cliente deverá remunerar a TeamViewer com uma compensação adequada pelo esforço decorrente dessa assistência, se e na medida em que tal for permitido pelas leis de proteção de dados aplicáveis.

2.7 Registros de atividades de processamento

A TeamViewer fornecerá ao Cliente as informações necessárias para manter os registros das atividades de processamento.

2.8 Data Deletion

At the choice of the Customer, TeamViewer shall delete or return the personal data that is processed on behalf of the Customer, if and to the extent that the law of the European Union or a member state to which TeamViewer is subject does not provide for an obligation to store the personal data.

2.9 Assistance with demonstration of DPA compliance

TeamViewer shall provide the Customer with all information necessary to demonstrate compliance with the obligations resulting from Sections 2 and 3 of this DPA. TeamViewer will also provide certificates of regular audits by recognized auditors or other qualified third parties, if required.

If and insofar there are objectively justified indications of a violation of this DPA or of data protection regulations by TeamViewer, TeamViewer will enable and contribute to additional audits, including inspections, which are carried out by the Customer or by a qualified auditor appointed by the Customer. When conducting the inspection, the Customer will not disrupt TeamViewer's operations in a disproportionate manner.

2.10 Notification of doubts regarding the instructions

TeamViewer shall inform the Customer immediately if TeamViewer is of the opinion that the execution of an instruction could lead to a violation of the applicable data protection law. TeamViewer is entitled to suspend the execution of the relevant instruction until it is confirmed in writing or changed by the Customer after the review.

2.11 Notification of breaches

If TeamViewer detects violations of the applicable data protection law, this DPA, or instructions of the Customer regarding the commissioned processing of personal data, TeamViewer shall inform the Customer immediately.

2.8 Exclusão de dados

A critério do Cliente, a TeamViewer deverá apagar ou devolver os dados pessoais que são processados em nome do Cliente, se e na medida em que a legislação da União Europeia ou de um Estado-Membro ao qual a TeamViewer esteja sujeita não preveja a obrigação de armazenar os dados pessoais.

2.9 Auxílio na demonstração de conformidade com a Adendo de Processamento de Dados (ADP)

A TeamViewer fornecerá ao Cliente todas as informações necessárias para demonstrar a conformidade com as obrigações decorrentes das Seções 2 e 3 deste Adendo de Processamento de Dados (ADP). A TeamViewer também fornecerá certificados de auditorias regulares realizadas por auditores reconhecidos ou outras terceiras partes qualificadas, se necessário.

Caso existam indícios objetivamente justificados de violação deste Adendo de Processamento de Dados (ADP) ou das normas de proteção de dados por parte da TeamViewer, a TeamViewer E contribuirá para auditorias adicionais, incluindo inspeções, realizadas pelo Cliente ou por um auditor qualificado por ele indicado. Ao realizar a inspeção, o Cliente não deverá interromper as operações da TeamViewer de forma desproporcional.

2.10 Notificação de dúvidas sobre as instruções

A TeamViewer informará o Cliente imediatamente caso considere que a execução de uma instrução possa levar a uma violação da legislação de proteção de dados aplicável. Reserva-se o direito de suspender a execução da instrução em questão até que esta seja confirmada por escrito ou alterada pelo Cliente após análise.

2.11 Notificação de violações

Caso a TeamViewer detecte violações da legislação de proteção de dados aplicável, deste Adendo de Processamento de Dados (ADP) ou das instruções do Cliente relativas ao processamento de dados pessoais contratado, a TeamViewer informará o Cliente imediatamente.

2.12 Data protection officer

TeamViewer has appointed an external data protection officer, who can be reached at privacy@teamviewer.com, or at TeamViewer Germany LLC, for the attention of the Data Protection Officer, Bahnhofplatz 2, 73033 Goppingen, Germany.

2.13 Data transfers to a third country

TeamViewer will generally only transfer personal data processed within the scope of this DPA to a country outside the EU or the European Economic Area (**EEA**) for which no adequacy decision of the EU Commission in the sense of Art. 45(3) GDPR exists (**unsafe third country**), provided that:

- a. the Customer or the Customer's user gives TeamViewer instructions for such a transfer, e.g., by requesting TeamViewer to establish a connection to an endpoint located in an unsafe third country (in such cases the Customer is responsible for ensuring that the data transfer is carried out in accordance with Art. 44 et seq. GDPR), or
- b. TeamViewer is obliged to do so according to the law of the European Union or a member state to which TeamViewer is subject; in such a case TeamViewer will inform the Customer about these legal requirements prior to processing, unless the respective law prohibits such a communication on important grounds of public interest.

Furthermore, TeamViewer shall be entitled to utilize Subprocessors in a third country to process personal data, insofar as the requirements of Art. 44 GDPR are met.

3 Subprocessors

3.1 Authorized Subprocessors

TeamViewer utilizes the services of a number of another processors (hereinafter, "**Subprocessors**"). The list of Subprocessors used by TeamViewer for each of the

2.12 Encarregado da proteção de dados

A TeamViewer nomeou um encarregado de proteção de dados externo, que pode ser contactado pelo endereço privacy@teamviewer.com, ou para TeamViewer Germany GmbH, aos cuidados do Encarregado da Proteção de Dados, Bahnhofplatz 2, 73033 Goppingen, Alemanha.

2.13 Transferências de dados para um país terceiro

Em geral, a TeamViewer só transferirá dados pessoais processados no âmbito desta Adendo de Processamento de Dados (ADP) para um país fora da UE ou do Espaço Econômico Europeu. (**EEE**) para a qual não existe decisão de adequação da Comissão Europeia nos termos do Artigo 45(3) do RGPD. existe. (**país terceiro inseguro**), desde que:

- a. o Cliente ou o usuário do Cliente fornece instruções à TeamViewer para tal transferência, por exemplo, solicitando à TeamViewer que estabeleça uma conexão com um terminal localizado em um país terceiro não seguro (nesses casos, o Cliente é responsável por garantir que a transferência de dados seja realizada de acordo com o Art. 44 e GDPR), ou
- b. A TeamViewer é obrigada a fazê-lo de acordo com a legislação da União Europeia ou de um Estado-Membro ao qual esteja sujeita; nesse caso, a TeamViewer informará o Cliente sobre esses requisitos legais antes do processamento, a menos que a respectiva legislação proíba tal comunicação por motivos importantes de interesse público.

Além disso, a TeamViewer terá o direito de utilizar subcontratados em um país terceiro para processar dados pessoais, desde que os requisitos do Art. 44 do sejam cumpridos.

3 Subprocessadores

3.1 Subprocessadores autorizados

O TeamViewer utiliza os serviços de vários outros processadores (doravante, "**Subprocessadores**"). A lista de subprocessadores usados pelo TeamViewer para cada

TeamViewer products can be found under the following link as [Annex 3](#). By concluding the DPA, the Customer agrees to the engagement of the Subprocessors that are included in [Annex 3](#) at the time of concluding the DPA for the relevant TeamViewer Product.

3.2 Appointment of new Subprocessors

If TeamViewer wishes to commission further or other Subprocessors to provide the contractually agreed services (e.g., hosting), such Subprocessors have to be selected with the required care and due diligence. TeamViewer shall notify the Customer at least fifteen (15) days in advance about the appointment of any new Subprocessors. The Customer has the right to object to the engagement of the Subprocessor by stating objectively comprehensible reasons. If no objection is raised within this period, the new Subprocessor notified accordingly shall be deemed approved. If, in the event of an objection within the deadline, no solution can be reached, either party is entitled to terminate the DPA with a notice period of two (2) weeks. When the termination of the DPA becomes effective, the EULA shall also be considered terminated. Reference is made to section B.5.5 (Consequences of termination) of the EULA.

3.3 Subprocessors in third countries

Subprocessors in third countries may only be engaged if the special requirements of Art. 44 et seq. GDPR are fulfilled.

3.4 Obligations of Subprocessors

TeamViewer shall structure the contracts with Subprocessors in a way that they comply with the requirements of the applicable data protection laws and this DPA and shall oblige the Subprocessors to commission additional or different Subprocessors with the processing of personal data when observing the provisions of section 3.2 towards TeamViewer. TeamViewer shall contractually impose obligations on the Subprocessors providing sufficient warranties that the appropriate technical and organizational measures will be implemented in such a way that the processing is carried out in accordance with the

um dos produtos TeamViewer pode ser encontrada no seguinte link: [Anexo 3](#). Ao celebrar o Adendo de Processamento de Dados (ADP), o Cliente concorda com a contratação dos Subprocessadores incluídos no presente documento. [Anexo 3](#) no momento da conclusão do Adendo de Processamento de Dados (ADP) para o produto TeamViewer relevante.

3.2 Nomeação de novos subcontratados

Caso a TeamViewer deseje contratar outros Subprocessadores para fornecer os serviços contratualmente acordados (por exemplo, hospedagem), Subprocessadores deverão ser selecionados com o cuidado e a devida diligência necessários. A TeamViewer notificará o Cliente com Menos quinze (15) dias de antecedência sobre a nomeação de quaisquer novos Subprocessadores. O Cliente tem Direito de se opor à contratação do Subprocessador, apresentando razões objetivamente compreensíveis. Caso não haja objeção dentro Período, o novo Subprocessador notificado será considerado aprovado. Se, em caso de objeção dentro do prazo, nenhuma solução puder ser alcançada, qualquer Das partes poderá rescindir o Adendo de Processamento de Dados (ADP) com um aviso prévio de (2) semanas. Quando a rescisão do Adendo de Processamento de Dados (ADP) entrar em vigor, o EULA também será considerado rescindido. Consulte a seção B.5.5 (Consequências da rescisão) do EULA.

3.3 Subprocessadores em países terceiros

Os subcontratados em países terceiros só podem ser contratados se os requisitos especiais do 44 e seguintes RGPD forem cumpridos.

3.4 Obrigações dos Subprocessadores

A TeamViewer estruturará os contratos com os Subprocessadores de forma a cumprir os requisitos das leis de proteção de dados aplicáveis e deste Adendo de Processamento de Dados (ADP) , e obrigará os Subprocessadores a contratar outros Subprocessadores, adicionais ou diferentes, para o processamento de dados pessoais, observando as disposições Seção 3.2 em relação à TeamViewer. A TeamViewer imporá contratualmente obrigações aos Subprocessadores, fornecendo garantias suficientes de que as medidas técnicas e organizacionais adequadas serão implementadas de forma a que o

requirements of the GDPR and this DPA.

4 Changes to this DPA

TeamViewer is generally entitled to amend the provisions of this DPA. TeamViewer will inform the Customer about the planned change and the content of the new DPA at least twenty-eight (28) days before such changes become effective. The change is considered approved if the Customer does not object to TeamViewer within fifteen (15) days after receipt of this information. If the Customer objects to the change, the DPA continues under the existing conditions.

5 Liability

Reference is made to Art. 82 of the GDPR.

For the rest, it is agreed that the regulations on limitation of liability from the corresponding license agreement shall apply.

6 Specific Terms for Regional Restricted Access

For the specific Product(s) "Regional Restricted Access" in the Contract, TeamViewer shall process personal data of Customer under this DPA within the United States. Processing outside the United States may occur: (i) to the extent necessary for maintenance, support, or development purposes, and as described in the then-current [Privacy Notices](#); (ii) upon request by Customer, specifically where Customer uses Services from a location outside the United States

processamento seja realizado em conformidade com os requisitos do RGPD e deste Adendo de Processamento de Dados (ADP).

4 Alterações a este Adendo de Processamento de Dados (ADP)

A TeamViewer geralmente tem o direito de alterar as disposições deste Adendo de Processamento de Dados (ADP). TeamViewer informará o Cliente sobre a alteração planejada e o conteúdo do novo Adendo de Processamento de Dados (ADP) com pelo menos vinte e oito (28) dias de antecedência da entrada em vigor das alterações. A alteração será considerada aprovada se o Cliente não apresentar objeção à TeamViewer dentro de quinze (15) dias após o recebimento desta informação. O presente objeção à alteração, o Adendo de Processamento de Dados (ADP) continuará em vigor nas condições existentes.

5 Responsabilidade

Faz-se referência ao 82 do RGPD.

No mais, fica acordado que se aplicarão as normas de limitação de responsabilidade constantes no respectivo contrato de licença.

6 Termos específicos para acesso regional restrito

Para o(s) Produto(s) específico(s) com "Acesso Regional Restrito" no Contrato, a TeamViewer processará os dados pessoais do Nos Estados Unidos, conforme este Adendo de Processamento de Dados (ADP). O processamento fora dos Estados Unidos poderá ocorrer: (i) na medida necessária para fins de manutenção, suporte ou desenvolvimento, e conforme descrito no DPA vigente, [Avisos de Privacidade](#); (ii) mediante solicitação do Cliente, especificamente quando o Cliente utiliza os Serviços de um localização fora dos Estados Unidos.

Annex 1 to the Data Processing Agreement

Details of Data Processing - TeamViewer products

Version as of March 9, 2026

Anexo 1 ao Data Processing Agreement

Detalhes do Processamento de Dados - Produtos TeamViewer

Versão de 9 de março de 2026

Content / Conteúdo

1	Subject 3 / Assunto -----	3
2	Duration / Duração	3
3	Nature and purpose of the processing 3 / Natureza e finalidade do tratamento	3
4	Type of personal data / Tipo de dados pessoais _____	7
5	Categories of data subjects / Categorias de titulares de dados	14
	Appendix - Engage/Co-Browsing to Exhibit 1 / Engage/Co-Browsing — Anexo 1	16
	Appendix - Classroom to Annex 1 / Da Sala de Aula para o Anexo 1 _____	18

ENGLISH

PORTUGUÊS

1 Subject

The general subject of data processing is described in the [EULA](#) as well as in the relevant [Product Specification](#).

2 Duration

The duration of the data processing corresponds to the duration of the [EULA](#).

3 Nature and purpose of the processing

TeamViewer will process personal data as the Customer's Processor in order to enable the use of the Software and Services as defined under the [EULA](#) according to documented instructions (in accordance with the product functionality) of the Customer and/or its users. This essentially covers the processing of the transmitted content as well as the organization of the contents of the user account.

When using the respective TeamViewer products, TeamViewer will carry out the processing activities on behalf of the Customer as set out below.

The further specification of the Software and Services is provided under the [Product Specification Page](#). Processing outside the scope of this DPA is described in the [Product Privacy Notice](#).

1 Assunto

O tema geral do processamento de dados é descrito em [EULA](#) bem como no contexto relevante [Especificações do produto](#).

2 Duração

A duração do processamento de dados corresponde à duração do [EULA](#).

3 Natureza e finalidade do processamento

A TeamViewer processará os dados pessoais como Processadora do Cliente para permitir o uso do Software e dos Serviços, conforme definido no contrato [EULA](#). De acordo com as instruções documentadas (em conformidade com a funcionalidade do produto) do Cliente e/ou seus usuários. Isso abrange essencialmente o processamento do conteúdo transmitido, bem como a empresa do conteúdo da conta do usuário.

Ao utilizar os respectivos produtos TeamViewer, a TeamViewer realizará as atividades de processamento em nome do Cliente, conforme descrito abaixo.

A especificação completa do Software e dos Serviços é fornecida em [link para a documentação], [Página de especificações do produto](#). O processamento fora do escopo deste Adendo de Processamento de Dados (ADP) é descrito no [Política de privacidade do Produto](#).

Product	Nature and Purpose of the Processing	Produto	Natureza e propósito do processamento
All TeamViewer products (except Frontline, Assist AR, Engage/Co-Browsing function module and Classroom, see separate section below)	<ul style="list-style-type: none"> - Processing of the data that the user enters into the user account, in particular storage and making it accessible to other users in the context of the connection e.g., name, contacts, email address, profile picture, as well as content data of the connections (e.g., chat). - Processing of contacts stored in the user's account, e.g., contact lists. - Transmission of the content data from the respective user to other users within a remote connection (e.g., desktop image, transmitted data and files as well as any other information exchanged). - Processing of data in the context of company profile management, such as licensed devices, rules, administration of the company profile, distribution of company policies, user access management, connection reports, Wake on LAN feature, etc. 	Todos os produtos TeamViewer (exceto Frontline, Assist AR, módulo de função Engage/Co-Browsing e Classroom, veja a seção separada abaixo)	<ul style="list-style-type: none"> - Processamento dos dados que o usuário insere na conta do usuário , em particular- armazenamento local e disponibilização desses dados a outros usuários no contexto da conexão , como nome, contatos, endereço de e-mail, foto de perfil, bem como dados de conteúdo das conexões (por exemplo, bate-papo). - Processamento de contatos armazenados na conta do usuário, por exemplo, listas de contatos. - Transmissão de dados de conteúdo do respectivo usuário para outros usuários. dentro de uma conexão remota (por exemplo, imagem da área de trabalho, dados e arquivos transmitidos, bem como quaisquer outras informações trocadas). - Processamento de dados no contexto da gestão do perfil da empresa, como por exemplo: Dispositivos licenciados, regras, administração do perfil da empresa, distribuição de políticas da empresa, gerenciamento de acesso de usuário , relatórios de conexão , recurso Wake-on-LAN , etc.
	<ul style="list-style-type: none"> - Transmission of the obfuscated client account data through the new security feature (if applicable). 		<ul style="list-style-type: none"> - Transmissão dos dados ofuscados da conta do client através da nova segurança- Recurso de ridade (se aplicável).
	<ul style="list-style-type: none"> - Processing of data in the context of meeting session planning e.g., start time, meeting topic, participants, meeting ID. 		<ul style="list-style-type: none"> - Processamento de dados no contexto do planejamento de sessão de reunião, por exemplo, início. Horário, tema da reunião, participantes, ID da reunião.
	<ul style="list-style-type: none"> - Processing data in the scope of the provision of an integration service. 		<ul style="list-style-type: none"> - Processamento de dados no âmbito da prestação de um serviço de integração.
	<ul style="list-style-type: none"> - Providing Customer and/or technical support. 		<ul style="list-style-type: none"> - Fornecer suporte ao cliente e/ou suporte técnico.
	<ul style="list-style-type: none"> - Providing Professional Services 		<ul style="list-style-type: none"> - Prestação de Serviços Profissionais
	<ul style="list-style-type: none"> - Provisioning of the Connection Report feature. - Allowing iOS in-app purchases and linking them to an account. - Processing of data in connection with your use of specific features or functions (available in the respective product depending on 		<ul style="list-style-type: none"> - Disponibilização da funcionalidade de Relatório de Conexão . - Permitir compras dentro do aplicativo iOS e vinculá-las a uma conta. - Processamento de dados em conexão com o seu uso de recursos ou funções específicos

	<p>your license), e.g.:</p> <ul style="list-style-type: none"> • Remote Monitoring, encompassing the monitoring of critical aspects of Customer's devices. • Network Device Monitoring, encompassing the monitoring of the availability and issues of network devices, such as routers, printers, etc. • Asset Management, Asset Management and Discovery, encompassing visibility of all Customers IT assets. • Patch Management, encompassing monitoring of vulnerabilities and patching of Customer's software and OS, as well as 3rd party applications. • Endpoint Protection, encompassing the protection of Customer's devices against viruses, trojans, spyware, ransomware etc. • Endpoint Protection/Endpoint Detection & Response, processing of personal data for the purpose of providing security and data protection services, enhancing threat defenses, and providing licenses to TeamViewer and endpoint protection/ endpoint detection and response products and services. • Device Management, processing of data for the purpose of providing mobile device management services. • Remote Scripting, which includes the creation, storage, deployment, and execution of scripts on remote devices. • Backup, encompassing the backup of Customer's business data. • Grafana Plugin, hosting service for providing Grafana 		<p>(disponíveis no respectivo produto, dependendo da sua licença), por exemplo:</p> <ul style="list-style-type: none"> • Monitoramento remoto, abrangendo o monitoramento de aspectos críticos dos dispositivos do Cliente. • Monitoramento de dispositivos de rede, Abrange o monitoramento da disponibilidade e dos problemas de dispositivos de rede, como roteadores, impressoras, etc. • Gerenciamento de ativos, Gerenciamento de ativos Visibilidade abrangente de todos os ativos de TI dos clientes. • Gerenciamento de patches, Abrangendo o monitoramento de vulnerabilidades e a aplicação de patches no software e no SO do cliente, bem como em aplicativos de terceiros. • Proteção de terminais, abrangendo a proteção dos dispositivos do Cliente contra vírus, cavalos de Troia, spyware, ransomware , etc. • Proteção de terminais / Detecção e resposta de Terminal processamento de Dados pessoais com a finalidade de fornecer serviços de segurança e proteção de dados, aprimorar as defesas contra ameaças e fornecer licenças para o TeamViewer e produtos e serviços de proteção de terminal / detecção e resposta de terminal . • Gerenciamento de Dispositivo , Processamento de dados com o objetivo de fornecer serviços de gerenciamento de dispositivo móvel . • Scripting remoto, que inclui a criação, o armazenamento e
--	--	--	---

	<p>PlugIn to the corresponding account, if desired by the Customer.</p> <ul style="list-style-type: none"> • Conditional Access, e.g., providing the Customer with a dedicated server. • REACH registry, processing data in context of the feature. • Meeting, processing of contacts stored in the user's address book to organize meetings, e.g., sending invitations, Outlook integration, and transmission of the content data entered by the respective user to other users within a meeting (image and sound as well as possible transmission of the data and files). • IoT, processing of sensor data with TeamViewer IoT cloud and subsequent transmission through the APIs. • Servicecamp/Service Desk, including but not limited to ticket contents, creation and assignment of the tickets, ticket reporting, ticket status, and service instance configuration parameters. • Automations, connecting TeamViewer data to a wide range of solutions. 		<p>a implantação, e execução de scripts em dispositivos remotos.</p> <ul style="list-style-type: none"> • Backup, abrangendo o backup dos dados comerciais do Cliente. • Plugin do Grafana, Serviço de hospedagem para disponibilizar o plugin Grafana na conta correspondente, caso seja do interesse do Cliente. • Acesso Condicional, Por exemplo, fornecer ao cliente um servidor dedicado. • Registro REACH, Processamento de dados no contexto da característica. • Meeting, processamento de contatos armazenados na agenda de endereços do usuário para organizar reuniões, por exemplo, enviando convites, integrando com o Outlook e transmitindo os dados de conteúdo inseridos pelo respectivo usuário para outros usuários dentro de uma reunião (imagem e som, bem como possível transmissão de dados e arquivos). • muito, processamento de dados de sensores com a nuvem TeamViewer IoT e subse- transmissão frequente através dos APLs. • Servicecamp/Central de Serviços, incluindo, mas não se limitando a, o conteúdo dos bilhetes, Criação e atribuição de tickets, geração de relatórios de tickets, status dos tickets e parâmetros de configuração da instância de serviço. • Automações, Conectando dados do TeamViewer a uma ampla gama de soluções.
<p>Frontline and Assist AR</p>	<p>Hosting of the login interface, as well as administration of relevant areas, such as users, devices, systems etc.</p> <p>- Setup of Frontline/Assist AR</p>	<p>Frontline e Assist AR</p>	<p>- Hospedagem da interface de login, bem como administração das áreas relevantes, tais como usuários, dispositivos, sistemas etc</p>

	<p>workplaces (mobile as well as wearable), including the device as well as user setup.</p> <ul style="list-style-type: none"> - Hosting and display of the dashboards as well as contact lists, asset management, workflow management and task deployment. - Provision of the built-in voice command recognition, if requested by the Customer. - Speech-to-text functionalities, including live captioning, transcription and translation. - Hosting of data in connection with Frontline xPick (e.g., pick-order management, workflow and task information, KPIs etc., including maintaining third-party components in workflows). - Hosting of the integration service, if requested by the Customer. - Transmission of the Frontline remote support calls. - Hosting of the remote support call recordings and remote call logs in connection with overall remote support administration, if requested by the Customer. - Services in the area of Halo-Lens technology, e.g., provision of eye-tracking functionality and augmented reality 3Dpoints. - Provision of support services, especially with regard to the customer feedback. - Hosting and management of Twilio console, if requested by the Customer. - Third level support for Customer's server instances, if requested by the Customer. - Transmission of the content data during the virtual remote support session (image, video, and sound as well as possible transmission of the data and files). - Enabling of a chat function, including the translation of chat content. - Provisioning the Optical Character Recognition (OCR) feature. 		<ul style="list-style-type: none"> - Configuração de estações de trabalho Frontline/ Assist AR (móveis e vestíveis), incluindo a configuração do dispositivo e do usuário . - Hospedagem e exibição de painéis de controle, listas de contatos, gerenciamento de ativos, gerenciamento de fluxo de trabalho e implantação de tarefas. - Disponibilização do recurso de reconhecimento de comandos de voz integrado, caso solicitado pelo Cliente. - Funcionalidades de conversão de voz em texto, incluindo legendagem ao vivo, transcrição e tradução. - Hospedagem de dados conexão ao Frontline xPick (por exemplo, gerenciamento de pedidos de coleta, informações de fluxo de trabalho e tarefas, KPIs etc., incluindo a manutenção de componentes de terceiros nos fluxos de trabalho). - Hospedagem do serviço de integração, caso solicitado pelo Cliente. - Transmissão das chamadas de suporte remoto da linha de frente. - Hospedagem das gravações de chamadas de suporte remoto e dos registros de chamadas remotas em conjunto com a administração geral do suporte remoto , caso solicitado pelo Cliente. - Serviços na área da tecnologia Halo-Lens, por exemplo, fornecimento de rastreamento ocular. Funcionalidade e realidade aumentada 3Dpoints. - Prestação de serviços de suporte, especialmente no que diz respeito ao feedback do cliente. - Hospedagem e gerenciamento do console Twilio, caso solicitado pelo Cliente. - Suporte de terceiro nível para instâncias de servidor do Cliente, se solicitado pelo Cliente.
--	--	--	---

	<ul style="list-style-type: none"> - Automated workflow creation with the PDF to Workflows feature. 		<ul style="list-style-type: none"> - Transmissão dos dados de conteúdo durante a sessão de suporte remoto virtual. (imagem, vídeo e som, bem como possível transmissão de dados e arquivos). - Ativação da função de bate-papo, incluindo a tradução do conteúdo do bate-papo. - Disponibilizando o recurso de Reconhecimento Óptico de Caracteres (OCR). - Criação automatizada de fluxos de trabalho com o recurso PDF para fluxos de trabalho.
Engage/Co-Browsing function module	<ul style="list-style-type: none"> - Provision of services within the scope of TeamViewer Engage/ Co-Browsing function module, including but not limited to hosting of the Customer data as well as maintenance and support services. - Provision of services within the scope of so-called video chat and live chat functionalities, including transmission and hosting of chat contents and other associated services, e.g., chatbots. - Provision of services within the scope of appointment scheduling and eSig-nature functionalities. - Provision of so-called software development kits (SDKs) for Customer applications enabling the integration of certain TeamViewer Engage/Co-Browsing functionalities within Customers own mobile apps (e.g., co-browsing, chats, etc.). 	Módulo de função Engage/Co-Browsing	<ul style="list-style-type: none"> - Prestação de serviços no âmbito do TeamViewer Engage/ Co-navegação módulo de funções, incluindo, entre outras coisas, o alojamento dos dados do cliente, bem como serviços de manutenção e suporte. - Prestação de serviços no âmbito do chamado bate-papo por vídeo e bate-papo ao vivo. funcionalidades, incluindo transmissão e hospedagem de conteúdo de bate-papo e outros serviços associados, como chatbots. - Prestação de serviços no âmbito do agendamento de consultas e assinatura eletrônica (eSig). funcionalidades da natureza. - Fornecimento dos chamados kits de desenvolvimento de software (SDKs) para aplicações do cliente. Aplicações que permitem a integração de determinadas funcionalidades do TeamViewer Engage/Co-Browsing nas aplicações móveis dos clientes (por exemplo, co-navegação, chats, etc.).
Classroom	<ul style="list-style-type: none"> - Provision of services within the scope of so-called video conference and live chat functionalities, including transmission and hosting of chat contents (including file transfer) and other associated services, e.g., conference notes. Provision of whiteboard, document sharing and tracking, polling, and breakout room 	Classroom	<ul style="list-style-type: none"> - Prestação de serviços no âmbito das chamadas funcionalidades de videoconferência e chat ao vivo, incluindo a transmissão e hospedagem de conteúdo de chat (incluindo transferência de arquivos) e outros serviços associados, como por exemplo, conferências. Observações. Oferecemos serviços de quadro branco,

	<p>services.</p> <p>Provision of account services including registration and account management</p>		<p>compartilhamento e acompanhamento de documentos, votação e salas de discussão.</p> <p>Prestação de serviços de conta, incluindo cadastro e gerenciamento de contas.</p>
AI services	<p>Provision of AI assisted features by processing user interactions during the session and data entered or generated (incl. resulting outputs), e.g., session summaries, categorization, tagging, capturing, summarizing, anonymizing, and hosting of the session data.</p>	Serviços de IA	<p>- Fornecimento de funcionalidades assistidas por IA através do processamento das interações do usuário durante a sessão e dos dados inseridos ou gerados (incluindo as saídas resultantes do "), como por exemplo, resumos de sessão , categorização, etiquetagem, captura, sumarização e anonimização. , e hospedagem dos dados da sessão .</p>
DEX services	<p>- Processing of personal data in connection with your use of DEX services, including but not limited to</p> <ul style="list-style-type: none"> • Endpoint Troubleshooting, providing visibility into and control over every endpoint. • Experience Analytics, using collected device data to monitor common friction factors that affect the digital workplace. • Endpoint Automation, encompasses endpoint management capabilities, e.g., reducing configuration drift, identifying incident root causes, and executing self-healing remediations. • Inventory Insights, normalizing inventory and hardware data into ven-dor, product, and version records for analytical and reporting purposes. • Application Experience Management, providing visibility of application experience by users and making a score for user experience evaluation available. • Patch Insights, providing an overview of the last mile patching required on Customer's environment. 	Serviços DEX	<p>- Processamento de dados pessoais conexão ao seu uso dos serviços DEX, incluindo, entre outros:</p> <ul style="list-style-type: none"> • Diagnóstico de endpoints, Proporcionando visibilidade e controle sobre cada terminal. • Análise de experiência, Utilizando dados coletados de dispositivo para monitorar fatores de atrito comuns que afetam o ambiente de trabalho digital. • Automação de endpoints, Abrange recursos de gerenciamento de terminal , como reduzir desvios de configuração, identificar as causas raiz de incidentes e executar correções de autorrecuperação. • Análises de estoque, normalizando dados de inventário e hardware em ven-Registros de dor, produto e versão para fins analíticos e de geração de relatórios. • Gestão da experiência do aplicativo, proporcionando visibilidade da aplicação experiência do usuário e disponibilização de uma pontuação para avaliação da experiência do usuário . • Informações sobre patches, fornecendo uma visão geral dos reparos finais necessários

	<ul style="list-style-type: none"> • Content Distribution, encompasses content delivery by utilizing bandwidth effectively enabling devices to share content locally, reducing redundancy. • Virtual Desktop Experience, providing proactive health management, and streamlining operations. • 1E Intelligence, multiplying IT's impact by merging edge and cloud AI for fast, precise, and deeply informed decisions and actions, e.g., Insights on emerging DEX issues, automated root-cause analyses, recommendation and remediation guidance. • 1E Catalog, curating data for Software or Hardware information for Vendor, Title, Colloquial, Version and Edition. • PXE Everywhere, allowing computers to automatically boot up into Windows PE to install Windows Operating System. • Processing personal data in the scope of provisioning integration services, such as Automated Self Service for ServiceNow (SCC (Service Catalog Connect) and Virtual Assistant), encompassing a set of advanced automation capabilities to extend the Service Catalog and Virtual Agent to instantly fulfill requests without making end users wait. • Service Desk Augmentation (ITSM Connect and 1E Core), providing real time incident investigation and remediation capabilities inside of ServiceNow. • CMDB Connector, providing the Device details to ServiceNow's CMDB. 		<p>no ambiente do cliente.</p> <ul style="list-style-type: none"> • Distribuição de conteúdo, Abrange a distribuição de conteúdo através da utilização eficaz da largura de banda, permitindo que os dispositivos compartilhem conteúdo localmente e reduzindo a redundância. • Experiência de Área de Trabalho Virtual, Oferecendo gerenciamento proativo de saúde, e otimizando as operações. • Inteligência 1E, Multiplicando o impacto da TI ao combinar IA de ponta e em nuvem para Decisões e ações rápidas, precisas e profundamente informadas, como por exemplo, insights sobre problemas emergentes no mercado de DEX, análises automatizadas de causa raiz, recomendações e orientações para correção. • Catálogo 1E, Curadoria de dados para informações de software ou hardware, incluindo fornecedor, título, nome coloquial, versão e edição. • PXE em todos os lugares, permitindo computadores para inicializar automaticamente no Windows PE para instalar o sistema operacional Windows. • Processamento de dados pessoais no âmbito da prestação de serviços de integração, tais como: • Autoatendimento automatizado para ServiceNow (SCC (Service Catalog Connect) e Assistente Virtual), Abrangendo um conjunto de recursos avançados de automação para estender o Catálogo de Serviços e o
--	---	--	---

	<ul style="list-style-type: none"> • Service Graph Connector, providing Device and Software details to ServiceNow CMDB. <p>- Provisioning of SaaS solutions, e.g.,</p> <ul style="list-style-type: none"> • Intune, providing mobile device management (MDM) and mobile application management (MAM) to control device usage and manage applications on company-owned and personal devices. • Device Refresh, optimizing device refresh strategies on devices. • Business Impact, processing data when opening incident tickets in an ITSM solution or offloading data to other solutions like Splunk. • Software Reclaim, providing an overview of software inventory usage to unused or rarely used software from your organization's endpoints 		<p>Agente Virtual, permitindo atender solicitações instantaneamente, sem fazer com que os usuários finais esperem.</p> <ul style="list-style-type: none"> • Aumento da Central de Serviços (ITSM Connect e 1E Core), Oferecendo recursos de investigação e remediação de incidentes em tempo real dentro do ServiceNow. • Conector CMDB, Fornecer os detalhes do Dispositivo ao CMDB do ServiceNow. • Conector de gráfico de serviço, Fornecer detalhes do Dispositivo e do software ao ServiceNow CMDB. <p>- Provisionamento de soluções SaaS, por exemplo,</p> <ul style="list-style-type: none"> • Tune, Fornecendo gerenciamento de dispositivo móvel (MDM) e gerenciamento de aplicativos móveis (MAM) para controlar o uso de dispositivo e gerenciar aplicativos em dispositivos corporativos e pessoais. • Atualização do Dispositivo, Otimizando estratégias de atualização de dispositivo . • Impacto nos negócios, processamento de dados ao abrir chamados de incidentes em um Solução ITSM ou descarregamento de dados para outras soluções como o Splunk. • Recuperação de Software, fornecendo uma visão geral do uso do inventário de software para Software não utilizado ou raramente utilizado dos endpoints da sua organização.
--	---	--	---

ENGLISH

PORTUGUÊS

4 Type of personal data

The following types of personal data are processed by TeamViewer as a Processor:

4 Tipo de dados pessoais

Os seguintes tipos de dados pessoais são processados pela TeamViewer na qualidade de Processadora:

Product	Nature and Purpose of the Processing	Produto	Natureza e propósito do processamento
All TeamViewer products (except Frontline, Assist AR, Engage/Co-Browsing function module and Classroom, see below)	<ul style="list-style-type: none"> - Content data exchanged between TeamViewer clients during a connection session, e.g., video and audio stream (screen views and user camera), file transfers, text chat, remote control commands, ticket content, whiteboard, as well as personal data required for the establishing of the connection. - User account information, e.g., TeamViewer ID, username, display name, email, IP address, profile picture (optional), language preference, meeting ID, location, password. The domain of the client as well as the account age (e.g., "older than 6 months") will be shown to the session host before connection as part of our Showing Supporter Data During Connection security feature. 	Todos os produtos TeamViewer (exceto Frontline, Assist AR, módulo de função Engage/Co-Browsing e Classroom, veja abaixo)	<ul style="list-style-type: none"> - Dados de conteúdo trocados entre clientes TeamViewer durante uma conexão . sessão, por exemplo, fluxo de vídeo e áudio (visualizações de tela e câmera do usuário), transferências de arquivos, bate-papo por texto, comandos de controle remoto, conteúdo de tickets, quadro branco, bem como dados pessoais necessários para o estabelecimento da conexão. - Informações da conta do Usuário , por exemplo, ID do TeamViewer, nome de usuário, nome de exibição, e-mail, endereço IP, foto de perfil (opcional), idioma preferido, ID da reunião, localização, senha. O domínio do client , bem como a idade da conta (por exemplo, "mais de 6 meses"), serão exibidos ao host da sessão antes da conexão, como parte do nosso recurso de segurança "Exibição de Dados do Usuário Durante a Conexão ".
	<ul style="list-style-type: none"> - User account management and administration data, e.g., user profile storing and sharing, account details, contact list, contact information, chat history, file attachment. 		<ul style="list-style-type: none"> - Dados de gerenciamento e administração de contas de Usuário , por exemplo, armazenamento de perfil de usuário . Envio e compartilhamento, detalhes da conta, lista de contatos, informações de contato, histórico do bate-papo, anexos de arquivos.
	<ul style="list-style-type: none"> - Company profile administration and management data, e.g., company profile, company policies, associations with user accounts, user access management, connection reports. 		<ul style="list-style-type: none"> - Dados de administração e gestão do perfil da empresa, por exemplo, perfil da empresa. Arquivos, políticas da empresa, associações com contas de usuário , gerenciamento de acesso de usuário , relatórios de conexão .
	<ul style="list-style-type: none"> - Personal data processed in context of functionalities (available depending on your license), including without limitation: customized modules; push notifications as initiated by the users; mailing services (e.g., 		<ul style="list-style-type: none"> - Dados pessoais processados no contexto de funcionalidades (disponíveis dependendo da sua licença), incluindo, entre outros: módulos personalizados; notificações push iniciadas pelos usuários; serviços de e-mail (por

	<p>notifying, updating, and reporting parameters as defined by the Customer); password reset (e.g., hosting account reset and mailing service, email with reset link, assignment of the new password to the account) as well as trusted device management (e.g., email notifications to prevent misuse of a device for login); audit logs to track changes from the user.</p> <ul style="list-style-type: none"> - Connection data stored locally on the user's device (log files, txt-files with the connections). - Personal data processed in the scope of an integration service (e.g., connection data, ticket content, etc.). - Personal data processed in the scope of Customer and/or technical support. - Personal data processed in the scope of Professional Services - Personal data displayed in the Connection Report (device data, text, image, audio, video and metadata of the session). - iOS in-app purchase data and subscription expiration date. - Personal data processed in connection with your use of specific features or functions (available in the respective product depending on your license), e. g.: <ul style="list-style-type: none"> • Remote Monitoring: Device information (e.g., device name, machine name, disk space, online state, event, CPU usage etc. as described in Product Specifications); Historic alert data per device (e.g., suspicious alerts or events as defined by the Customer's individual settings; Scripting data (e.g., device name, user credentials, executed scripts per device depending on how the Customer chooses to execute the script); Content of the connections between the management console and managed devices. The content data is always encrypted, and 		<p>exemplo, atualizações, notificações, parâmetros de configuração e relatório conforme definidos pelo Cliente); redefinição de senha (por exemplo, redefinição da conta de hospedagem e serviço de e-mail, e-mail com link de redefinição, atribuição da nova senha à conta), bem como gerenciamento de dispositivo confiável (por exemplo, notificações e-mail para evitar o uso indevido de um dispositivo para login); registros de auditoria para rastrear alterações do usuário.</p> <ul style="list-style-type: none"> - Os dados de Conexão são armazenados localmente no dispositivo do usuário (arquivos de log, arquivos .txt com as conexões). - Dados pessoais tratados no âmbito de um serviço de integração (ex.: dados de conexão, conteúdo do bilhete, etc.). - Dados pessoais tratados no âmbito do suporte ao cliente e/ou suporte técnico. - Dados pessoais processados no âmbito de Serviços profissionais - Dados pessoais exibidos no Relatório de Conexão (dados do dispositivo, texto, imagem, áudio, vídeo e metadados da sessão). - Dados de compras no aplicativo iOS e data de expiração da assinatura. - Dados pessoais processados em conexão com o seu uso de recursos ou funções específicos (disponíveis no respectivo produto, dependendo da sua licença), por exemplo. g.: <ul style="list-style-type: none"> • Monitoramento remoto: Informações do Dispositivo (por exemplo, nome do dispositivo, nome da dispositivo, espaço em disco, estado online, evento, uso da CPU etc. conforme descrito nas Especificações do Produto); Dados históricos de alertas por dispositivo (por exemplo, alertas ou eventos Conforme definido pelas
--	--	--	---

	<p>TeamViewer can never access any of the content; Error log data stored on the user's device; Information in connection with customized individual monitoring policies.</p> <ul style="list-style-type: none"> • Asset Management, Asset Management and Discovery: Device information (e.g., type of the devices, device name, disk space, hardware details, installed software etc. as described in Product Specifications); and discovering devices in the network through scanner. • Patch Management: Device information (e.g., type of the devices, device name, machine name, disk space, online state, event, CPU usage, installed software etc. alongside with the executed patches per device. • Endpoint Protection: Device information alongside the security and anti-virus protection alerts per device as well as historic alert data (affected device, malware type, date etc.). • Endpoint Protection/Endpoint Detection & Response: Contact information, IP address and device information, License data, machine and user specific data, location data, and other data required to provide the service. Some data will be processed to improve threat identification as part of the service. • Mobile Device Management: certain license information, your name, email address, username, IP address, meta data, location data, login credentials and mobile device data and similar in order to activate your license, respectively link it to your account and for the use of mobile device management more broadly. In addition, data 		<p>configurações individuais do Cliente); Dados de scripts (por exemplo, nome do dispositivo , credenciais do usuário , scripts executados por dispositivo , dependendo de como o Cliente optar por executar o script); Conteúdo das conexões entre o console de gerenciamento e os dispositivos gerenciados. Os dados de conteúdo são sempre criptografados e o TeamViewer nunca pode acessar nenhum conteúdo; Dados de log de erros armazenados no dispositivo do usuário; Informações conexão a políticas de monitoramento individuais personalizadas.</p> <ul style="list-style-type: none"> • Gerenciamento de ativos, Gerenciamento de ativos : Informações do Dispositivo informações (por exemplo, tipo de dispositivo , nome do dispositivo , espaço em disco, detalhes de hardware, software instalado etc. conforme descrito nas Especificações do Produto); e descoberta de dispositivos na rede por meio do scanner. • Gerenciamento de patches: Informações do Dispositivo (por exemplo, tipo de dispositivo, dispositivo) Nome, nome da dispositivo , espaço em disco, estado online, evento, uso da CPU, software instalado etc. junto com os patches executados por dispositivo. • Proteção de terminais: Informações do Dispositivo , juntamente com a segurança e Alertas de proteção antivírus por dispositivo , bem como dados históricos de alertas (dispositivo afetado, tipo de malware , data etc.). • Proteção de terminais / Detecção e resposta de Terminal : Informações de contato informações sobre o
--	---	--	---

	<p>changed through linked 3rd party accounts may be synced with your TeamViewer account and merged with data in the TeamViewer service.</p> <ul style="list-style-type: none"> • Backup: Any data that the Customer chooses to back up, e.g., various files and folders that may include personal data. All data is encrypted, and only the Customer is able to download and decrypt the content from the backup. The creation, storage, recovery, and deletion of backups is executed in line with the parameters defined by the Customer. • IoT: Content data exchanged between TeamViewer clients during an IoT connection session (e.g., file transfers, remote control commands); data in connection with sensor management, e.g., IoT sensor information (Sensor ID, sensor names, metric names, metric value type (i.e., Celsius, kilogram, meter), data type (text, number, etc.) as well as IoT API credentials (e.g., certificates and credentials used to authenticate IoT devices to push IoT sensor data); data in connection with the analysis, visualization and setting of the measurements from sensors as well as processing of this data in the TeamViewer IoT cloud managed and adjusted by the Customer. • Meeting: subject of meeting, time zone, meeting ID, meeting start time, meeting end time; meeting scheduling and outlook integration (e.g., time and date of meetings, participants etc.); user account information (TeamViewer ID, username, IP address, profile picture, language settings, meeting ID, location, password). • Service Camp/Service Desk: 		<p>dispositivo , endereço IP e informações da licença, dispositivo e</p> <p>Dados específicos do usuário , dados de localização e outros dados necessários para fornecer o Serviço. Alguns dados serão processados para melhorar a identificação de ameaças como parte do serviço.</p> <ul style="list-style-type: none"> • Gerenciamento de dispositivos móveis: Certas informações da licença, seu nome, endereço de e-mail, nome de usuário, endereço IP, metadados, dados de localização , credenciais de login e dados do dispositivo móvel , entre outros, são coletadas para ativar sua licença, vinculá-la à Conta e para o gerenciamento do dispositivo móvel em geral. Além disso, os dados foram alterados através de Contas de terceiros vinculadas podem ser sincronizadas com sua conta TeamViewer e mescladas com os dados do serviço TeamViewer. • Backup: Dados que o Cliente optar por backup, como arquivos e pastas diversos que podem conter dados pessoais. Todos os dados são criptografados e somente o Pode baixar e descriptografar o conteúdo do backup. A criação, o armazenamento, a recuperação e a exclusão de backups são executados de acordo com os parâmetros definidos pelo Cliente. • Muito: Dados de conteúdo trocados entre clientes TeamViewer durante uma sessão de conexão IoT (por exemplo, transferências de arquivos, comandos de controle remoto) dados conexão ao gerenciamento de sensores, como informações de sensores IoT (ID do sensor, nomes dos sensores, nomes
--	---	--	---

	<p>Personal data in connection with ticket processing and reporting (e.g., TeamViewer IDs, emails, ticket subjects, date and time of tickets, content of the tickets, assignees as well as parameters defined by the Customer); Hosting the ticket meta data (e.g., creation and closing date/time, status, assignee etc.); Personal data in connection with ticket reporting, e.g., location, status, priority, assignee, average resolution times, user activities etc. as defined by the Customer.</p> <ul style="list-style-type: none"> • Remote Scripting: Device information, prompts, number of prompts over a timeframe, etc. • Web Monitoring: IP address, location data, response time, credentials, system status. • Automations: Depending on customer configuration, e.g. event logs, connection data, etc. 		<p>das métricas, tipo de valor da métrica (ou seja, Celsius, quilograma, metro), tipo de dados (texto, número etc.)), bem como credenciais da API IoT (por exemplo, certificados e credenciais usados para autenticar dispositivos IoT para enviar dados de sensores IoT); dados conexão à análise, visualização e configuração das medições dos sensores, bem como ao processamento desses dados na nuvem IoT do TeamViewer, gerenciada e ajustada pelo Cliente.</p> <ul style="list-style-type: none"> • Meeting: Assunto da reunião, fuso horário, ID da reunião, horário de início da reunião, Horário de término da reunião; agendamento de reuniões e integração com o Outlook (ex.: hora e data das reuniões, participantes etc.); informações da conta do usuário (ID do TeamViewer, nome de usuário, endereço IP, foto de perfil, configurações de idioma, ID da reunião, localização, senha). • Posto de Atendimento/Balcão de Atendimento: Dados pessoais conexão ao bilhete Processamento e geração de relatórios (por exemplo, IDs do TeamViewer, e-mails, assuntos dos tickets, data e hora dos tickets, conteúdo dos tickets, responsáveis, bem como parâmetros definidos pelo Cliente); Hospedagem dos metadados dos tickets (por exemplo, data/hora de criação e fechamento, status, responsável etc.); Dados pessoais conexão à geração de relatórios de tickets, por exemplo, localização, status, prioridade, responsável, tempos médios de resolução, atividades do usuário etc. conforme definido pelo • Scripting remoto: Informações do Dispositivo, avisos, número de avisos ao
--	---	--	--

			<p>longo de um período de tempo, etc.</p> <ul style="list-style-type: none"> • Monitoramento da Web: Endereço IP, dados de localização, tempo de resposta, credenciais, status do sistema. • Automações: Dependendo da configuração do cliente, por exemplo, logs de eventos conexão- dados de conexão, etc.
<p>Frontline</p>	<p>User account data (e.g., email, password, domain, IP address, profile picture, display name, phone number, roles and permissions, team name, role, organization, language, status (online/offline), 2-factor authentication, phonebook information).</p> <ul style="list-style-type: none"> - Personal data in connection with the initiated session, e.g., session ID, security tokens (login and refresh), IP address, username, start time, device information, session validity, as well as exchanged content. - Personal data in connection with the used device which enables the user to use Frontline, e.g., device ID, name, IP address, username, application version, Bluetooth MAC address, device firmware version, device logs, step counts and the achievement count (if available). - Personal data in connection with the calls made using the devices using xAssist. e.g., ID, username, team name, call link and title, start/end time and date, call event logs, multimedia asset information (video, image, text, sound etc.), call status. - Personal data in connection with the workflows, e.g., IDs, title, creation/update time and date, owner, step entry information, version number, tags. - Personal data in connection with service reports, e.g., call details, title, in-ternal number, date/time, description, status. - Personal data in connection with 	<p>Frontline</p>	<ul style="list-style-type: none"> - Dados da conta do Usuário (por exemplo, e-mail, senha, domínio, endereço IP, foto de perfil, Exibir nome, número de telefone, funções e permissões, nome da equipe, função, organização, idioma, status (online/offline), autenticação de dois fatores. (Informações da lista telefônica). - Dados pessoais conexão à sessão iniciada, como ID da sessão, tokens de segurança (login e atualização), endereço IP, nome de usuário, horário de início, informações do dispositivo, validade da sessão, bem como conteúdo trocado. - Dados pessoais conexão ao dispositivo utilizado que permite ao usuário usar o Frontline, como por exemplo, ID do dispositivo, nome, endereço IP, nome de usuário, versão do aplicativo, endereço MAC do Bluetooth, versão do firmware do dispositivo, registros do dispositivo, contagem de passos e contagem de conquistas (se disponível). - Dados pessoais conexão às chamadas feitas usando os dispositivos com o xAssist. exemplo: ID, nome de usuário, nome da equipe, link e título da chamada, hora e data de início/término, logs de eventos da chamada, informações de recursos multimídia (vídeo, imagem, texto, som etc.), status da chamada. - Dados pessoais conexão aos fluxos de trabalho, como IDs, título, data e hora de criação/atualização, proprietário, informações de entrada de

	<p>assets, in particular, Frontline specific as-sets, incl. but not limited to workflows (.uwe), components (.uce), and application (.uab).</p> <ul style="list-style-type: none"> - Picking, article and system information as well as warehouse information, as long as they contain user data. - Personal data in connection with sensor information, if any (e.g., creator, user etc.). - Personal data in connection with tasks, if any (e.g., creator, user etc.). - Personal data in connection with set cookies, which allows for personaliza-tion and improvement of the products. - Personal data in connection with the speech-to-text features, e.g., personal Identifier (Account ID) as well as the audio content of the session. - Data processed in connection with the PDF to Workflows feature, including the up-loaded workflow document. 		<p>etapas, número da versão e tags.</p> <ul style="list-style-type: none"> - Dados pessoais conexão a relatórios de serviço, como detalhes da chamada, título, número interno, data/hora, descrição e status. - Dados pessoais conexão a ativos, em particular, dados específicos da Frontline, como: conjuntos, mas não se limitando a, fluxos de trabalho (.uwe), componentes (.uce) e aplicativos (.uab). - Informações sobre separação de pedidos, artigos e sistemas, bem como informações sobre o armazém. contanto que contenham dados do usuário . - Dados pessoais conexão com informações de sensores, se houver (por exemplo, criador, usuário etc.). - Dados pessoais conexão com as tarefas, se existirem (ex.: criador, usuário , etc.). - Dados pessoais conexão a cookies definidos, que permitem a personalização. ção e aprimoramento dos produtos. - Dados pessoais conexão com as funcionalidades de conversão de voz em texto, por exemplo, dados pessoais Identificador (ID da conta), bem como o conteúdo de áudio da sessão. - Dados processados em conexão com o recurso PDF para Fluxos de Trabalho, incluindo o up-Documento de fluxo de trabalho carregado.
Assist AR	<ul style="list-style-type: none"> - Personal data in connection with the initiated session, e.g., session ID, secu-rity tokens (login and refresh), IP address, username, device information, session validity, as well as transferred stream (video and audio feeds), file transfers, text chat, remote control commands, ticket content, whiteboard, team name, call link and title, start/end time and date, call event logs, chat logs, multimedia asset information (video, image, text, sound etc.), call sta-tus. - User account information, e.g., 	Assist AR	<ul style="list-style-type: none"> - Dados pessoais conexão à sessão iniciada, por exemplo, ID da sessão , segurança. Tokens de acesso (login e atualização), endereço IP, nome de usuário, informações do dispositivo , validade da sessão , bem como fluxo transferido (feeds de vídeo e áudio), transferências de arquivos, bate-papo por texto, comandos de controle remoto, conteúdo do ticket, quadro branco, nome da equipe, link e título da chamada, hora e data de início/término, logs de eventos da chamada, registros de bate-papo,

	<p>TeamViewer ID, username, display name, email, IP address, profile picture (optional), language preference, tele-phone number(s), location, password.</p> <ul style="list-style-type: none"> - Personal data in connection with the user account management and administration, e.g., user profile storing and sharing, account details, buddy list, contact information, chat history, file attachments, password, domain, IP address, roles and permissions, status (online/offline), 2-factor authentication, phonebook information. - Personal data in connection with the company profile administration and management data, e.g., company profile, company policies, associations with user accounts, user access management. - Personal data transmitted during the TeamViewer Assist AR augmented reality video feed, as well as the hosting of the content. - Personal data in connection with the SMS product invite (e.g., phone number). - Push notifications as initiated by the users. - Personal data in connection with the speech-to-text features, e.g., personal Identifier (Account ID) as well as the audio content of the session, if activated by the user. - Personal data processed within the mailing services (e.g., notifying, updating, and reporting parameters defined by the Customer). - Personal data in connection with service reports, e.g., call details, title, internal number, date/time, description, status. - Personal data in connection with assets, in particular, Assist AR specific assets, incl. but not limited to application (.uab) assets. - Personal data in connection with password reset (e.g., hosting account reset and mailing service, email with reset link, assignment of the new password to the 		<p>informações de ativos multimídia (vídeo, imagem, texto, som etc.), status da chamada.</p> <ul style="list-style-type: none"> - Informações da conta do Usuário , por exemplo, ID do TeamViewer, nome de usuário, nome de exibição, e-mail, endereço IP, foto de perfil (opcional), idioma preferido, número(s) de telefone, localização, senha. - Dados pessoais conexão à gestão e administração da conta do usuário , como armazenamento e compartilhamento de perfil de usuário , detalhes da conta, lista de amigos, informações de contato, histórico de bate-papo, anexos de arquivos, senha, domínio, endereço IP, funções e permissões, status (online/offline), autenticação de dois fatores e informações da lista telefônica. - Dados pessoais conexão à administração e gestão do perfil da empresa, como por exemplo, perfil da empresa, políticas da empresa, associações com contas de usuário e gestão de acesso de usuário . - Os dados pessoais transmitidos durante a videoconferência de realidade aumentada do TeamViewer Assist AR , bem como a hospedagem do conteúdo. - Dados pessoais conexão ao convite do produto SMS (ex.: número de telefone). - Notificações push iniciadas pelos usuários. - Dados pessoais conexão com as funcionalidades de conversão de voz em texto, como por exemplo, o identificador pessoal (ID da conta), bem como o conteúdo de áudio da sessão, caso esta tenha sido ativada pelo usuário. - Dados pessoais processados no âmbito dos serviços de envio de correspondência (por exemplo, parâmetros de notificação, atualização e relatório definidos pelo Cliente). - Dados pessoais conexão a
--	--	--	---

	<p>account) as well as trusted device management (e.g., email notifications to prevent misuse of a device for login).</p> <ul style="list-style-type: none"> - Personal data required for Optical Character Recognition (OCR), including video data and session metadata. 		<p>relatórios de serviço, como detalhes da chamada, título, número interno, data/hora, descrição e status.</p> <ul style="list-style-type: none"> - Dados pessoais conexão a ativos, em particular, ativos específicos do Assist AR , mas não se limitando a, ativos de aplicativos (.uab). - Dados pessoais conexão à redefinição de senha (por exemplo, redefinição de conta de hospedagem e serviço de e-mail, e-mail com link de redefinição, atribuição da nova senha à conta), bem como gerenciamento de dispositivo confiável (por exemplo, notificações por e-mail para evitar o uso indevido de um dispositivo para login). - Dados pessoais necessários para o Reconhecimento Óptico de Caracteres (OCR), incluindo dados de vídeo e metadados da sessão .
<p>Engage/Co-Browsing function module</p>	<p>Personal Data processed in connection with the use of the functions:</p> <ul style="list-style-type: none"> - TeamViewer Co-Browsing: <ul style="list-style-type: none"> • IP address, which is collected when establishing a connection through Co-Browsing, since the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service Provider). • Depending on how and where a Customer uses Co-Browsing. If Co-Browsing is e.g., used during a checkout process, where the User can enter personal data such as name, email, address, payment information etc., then personal data can be made visible to the Agent. The sequences of User's keystrokes are not put into context to identify, structure, process, categorize, nor analyze the personal data 	<p>Módulo de função Engage/Co-Browsing</p>	<p>Dados pessoais tratados em conexão com a utilização das funcionalidades:</p> <ul style="list-style-type: none"> • Navegação conjunta do TeamViewer: • Endereço IP, que é coletado ao estabelecer uma conexão através de Navegação conjunta, já que o navegador e o servidor trocam endereços IP. Por padrão, o TeamViewer não armazena nem processa endereços IP, exceto para determinar a localização aproximada do Usuário por meio do Provedor de serviços de internet (ISP). • Dependendo de como e onde um Cliente usa a Co-Navegação. Se a Co-Navegação for usada, por exemplo, durante um processo de finalização de compra, onde o Usuário pode inserir dados pessoais como nome, e-mail, endereço, informações de pagamento etc., então esses dados pessoais podem ficar visíveis para o Agente. As sequências de teclas digitadas pelo Usuário não são contextualizadas para identificar, estruturar, processar, categorizar ou analisar os dados pessoais que possam conter (como nome, etc.). • Gravação de co-navegação, que pode incluir dados

	<p>they may contain (such as name, etc.).</p> <ul style="list-style-type: none"> Co-Browsing recording, which may include personal data as described in this section (optional). Personal data processed via so-called local storage variables and cook-ies, including the Session ID, acceptance of privacy policy (true/false). Such variables and cookies are by default set only for the duration of the session and are not used to re-identify the User at a later stage. More information on cookies and local storage variables is included as <u>Appendix - Engajar/Co-Browsing</u> below. User interactions, including mouse movements, clicks, scrolls, visited pages. Employee personal data, e.g., name, email, language, assigned Co-Browsing sessions, Co-Browsing recordings, number of Co-Browsing sessions, activity logs, status, average co-browsing and chat durations per Employee, initiated and accepted co-browsing sessions, declined sessions, ended sessions and similar depending on Customer preferences. Personal data included in various reports, including but not limited per-formance, statistical and similar reports. <p>- Live Chat, Video Chat, Chatbots</p> <ul style="list-style-type: none"> IP address, which is collected when a chat conversation is initiated, since the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service Provider). 		<p>pessoais conforme descrito em esta seção (opcional).</p> <ul style="list-style-type: none"> Dados pessoais processados através das chamadas variáveis de armazenamento local e scripts. Informações, incluindo o ID da Sessão , aceitação da política de privacidade (verdadeiro/falso). Essas variáveis e cookies são definidos por padrão apenas durante a duração do sessão e não são usadas para reidentificar o Usuário posteriormente. Mais informações sobre cookies e variáveis de armazenamento local estão incluídas como <u>Apêndice - Engajar/Navegação conjunta</u> abaixo. Interações do Usuário , incluindo movimentos do mouse, cliques, rolagem e páginas visitadas. Dados pessoais dos funcionários, como nome, e-mail, idioma, sessões de co-navegação atribuídas, gravações de co-navegação, número de sessões de co-navegação, registros de atividades, status, duração média de co-navegação e bate-papo por funcionário, sessões de co-navegação iniciadas e aceitas, sessões recusadas, sessões encerradas e similares, dependendo das preferências do cliente. Dados pessoais incluídos em diversos relatórios, incluindo, entre outros, relatórios de desempenho, estatísticos e similares. <p>- Chat ao vivo, Chat por vídeo, Chatbots</p> <ul style="list-style-type: none"> O endereço IP é coletado quando uma conversa de bate-papo é iniciada, já que o navegador e o servidor trocam endereços IP Por padrão, o TeamViewer não armazena nem processa endereços IP,
--	---	--	---

	<ul style="list-style-type: none"> • Personal data provided by users themselves, including but not limited to names, email addresses, phone numbers, invoice numbers, account numbers, financial information, attachments such as pictures, files, videos and similar. • Personal data relating to Live Chat, e.g., Session ID, browser and device information, or notices made by the Customer's Employees as well as chat recordings. • Personal data in connection with the video chat as initiated between the Customer's users and Customer's Employees, including audio and video transmission, as well as personal data in connection with their interaction, involving e.g., whiteboard, screen sharing, or documents, as applicable. • Personal data processed via so called local storage variables and cookies, including the Session ID, acceptance of privacy policy (true/false), interaction with chat. Such variables and cookies are by default set only for the duration of the session and may be used to re-identify the User at a later stage, depending on Customer's default configurations. More information on cookies and local storage variables are included as <u>Apêndice - Engajamento/Co-Navegação</u> below. • Chat history stored in the data center for a certain period of time by the Controller's Customers. • Employee personal data, e.g., name, email, language, assigned Chats, number of chats, activity logs, status, number of chats, chat durations per Employee, number of conversations by Employee and similar 		<p>exceto para determinar a localização aproximada do Usuário por meio do Provedor de serviços de internet (ISP).</p> <ul style="list-style-type: none"> • Dados pessoais fornecidos pelos próprios usuários, incluindo, entre outros, nomes, endereços e-mail, números de telefone, números de faturas, números de contas, informações financeiras, anexos como fotos, arquivos, vídeos e similares. • Dados pessoais relacionados ao chat ao vivo, como ID da Sessão, navegador e dispositivo. Informações ou avisos feitos pelos funcionários do cliente, bem como gravações de bate-papo. • Dados pessoais conexão ao bate-papo por vídeo iniciado entre o Usuários e funcionários do Cliente, incluindo transmissão de áudio e vídeo, bem como dados pessoais conexão à sua interação, envolvendo, por exemplo, quadro branco, compartilhamento de tela ou documentos, conforme aplicável. • Dados pessoais processados por meio de variáveis de armazenamento local e cookies, incluindo o ID da Sessão, aceitação da política de privacidade (verdadeiro/falso), interação com o chat. Essas variáveis e cookies são definidos por padrão apenas durante a sessão e podem ser usados para reidentificar o Usuário posteriormente, dependendo das configurações padrão do cliente. Mais informações sobre cookies e variáveis de armazenamento local estão incluídas como <u>Apêndice - Engajamento/Co-Navegação conjunta</u> abaixo. • O histórico de bate-papo é armazenado no centro de
--	--	--	--

	<p>depending on Customer's preferences. Further information may include how long did it take for an Employee to open an assigned chat, how much time did he spend reading the chat, how much time did he spend answer-ing (also how many text blocks/message templates did an employee use) etc. depending on Customer's default configurations.</p> <ul style="list-style-type: none"> • Personal data included in various dashboards and reports, including but not limited to performance, statistical and similar reports. 		<p>dados por um determinado período de tempo pelo Clientes do Controlador.</p> <ul style="list-style-type: none"> • Dados pessoais do funcionário, por exemplo, nome, e-mail, idioma, chats atribuídos, Número de chats, registros de atividades, status, número de chats, duração dos chats por funcionário, número de conversas por funcionário e similares, dependendo das preferências do cliente. Mais informações podem incluir: <ul style="list-style-type: none"> Quanto tempo levou para um funcionário abrir um chat atribuído? Quanto tempo ele gastou lendo o chat, quanto tempo gastou respondendo (e quantos blocos de texto/modelos de mensagem um funcionário usou), etc.? isso depende das configurações padrão do cliente. • Dados pessoais incluídos em diversos painéis e relatórios, incluindo, entre outros, relatórios de desempenho, estatísticos e similares. <p>- Agendador de consultas</p> <ul style="list-style-type: none"> • Informações de contato dos usuários do cliente (ex.: nome, endereço de e-mail, número de telefone). • Envio e hospedagem de confirmações e lembretes de consultas. • Hospedagem de informações e histórico de agendamentos. • Dados pessoais incluídos em diversos painéis e relatórios, incluindo, entre outros, relatórios de desempenho, estatísticos e similares.
<p>Classroom</p>	<p>- IP address, which is collected when a session with TeamViewer's services is established, this is because the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service</p>	<p>Classroom</p>	<p>- O endereço IP é coletado quando uma sessão com os serviços do TeamViewer é estabelecida, pois o navegador e o servidor trocam endereços Por padrão, o TeamViewer não armazena nem processa endereços IP, exceto para determinar a localização aproximada do Usuário por meio do Provedor de serviços de internet (ISP).</p>

	<p>Provider).</p> <ul style="list-style-type: none"> - Personal data provided by users themselves, including but not limited to names, email addresses, attachments such as pictures, files, videos and similar. - Personal data relating to the Video Conference session, e.g., Session ID, browser and device information, or notices made by the Customer's Employees as well as chat recordings. - Personal data in connection with the Video Conference as initiated between the Customer's users and Customer's Employees, including audio and video transmission, as well as personal data in connection with their interaction, involving e.g., whiteboard, screen sharing, or documents, as applicable. - Personal data processed via so called local storage variables and cookies, including the Session ID, acceptance of privacy policy (true/false), interaction with chat. Such variables and cookies are by default set only for the duration of the session and may be used to re-identify the User at a later stage, depending on the Customer's default configurations. More information on cookies and local storage variables is included as <u>Appendix-Classroom</u> below. - Chat history stored in the data center for a certain period of time by the Controllers Customers. - Employee personal data, e.g., name, email, or language, activity logs. - Video conference recordings if Customer chooses to record and store them 		<ul style="list-style-type: none"> - Dados pessoais fornecidos pelos próprios usuários, incluindo, entre outros, nomes, endereços e-mail, anexos como fotos, arquivos, vídeos e similares. - Dados pessoais relativos à sessão de videoconferência, como por exemplo, ID da Sessão, informações do navegador e do dispositivo, ou avisos feitos pelos funcionários do cliente, bem como gravações de bate-papo. - Dados pessoais conexão com a videoconferência iniciada entre os utilizadores do Cliente e os funcionários do Cliente, incluindo a transmissão de áudio e vídeo, bem como dados pessoais conexão com a sua interação, envolvendo, por exemplo, quadro branco, partilha de ecrã ou documentos, conforme aplicável. - Dados pessoais processados por meio de variáveis de armazenamento local e cookies, incluindo o ID da Sessão, aceitação da política de privacidade (verdadeiro/falso), interação com o chat. Essas variáveis e cookies são definidos por padrão apenas durante a sessão e podem ser usados para reidentificar o Usuário posteriormente, dependendo das configurações padrão do cliente. Mais informações sobre cookies e variáveis de armazenamento local estão incluídas em <u>Apêndice - Sala de aula</u> abaixo. - O histórico de bate-papo é armazenado no centro de dados por um determinado período de tempo pelo Controladores Clientes. - Dados pessoais dos funcionários, como nome, e-mail ou idioma, registros de atividades. - Gravações de videoconferências, caso o Cliente opte por gravar e armazenar.
AI Services	<ul style="list-style-type: none"> - User interactions during the session. - Data entered or generated, depending on the features in use 	Serviços de IA	<ul style="list-style-type: none"> - Interações do Usuário durante a sessão. - Dados inseridos ou gerados, dependendo das funcionalidades em uso.
DEX Services	<ul style="list-style-type: none"> - Device data processed by all DEX 	Serviços de DEX	<ul style="list-style-type: none"> - Dados do Dispositivo processados

	<p>services, including but not limited to device performance data, OS performance data, software performance and installation data, network data</p> <p>- Personal data processed in connection with your use of specific modules:</p> <ul style="list-style-type: none"> • Experience Analytics: usage data, e.g., device interaction data, browser interaction data and replies to user surveys. • Application Experience Management: software data e.g., software publisher and version, software interaction data, software crashes and hang data. • Virtual Desktop Experience: virtual desktop infrastructure data, including connection start and end timestamps. • 1E Intelligence: personal data including instruction metadata and author. • Patch Insights: missing and applied patches. • Integration services: e.g., device information, usernames. • SaaSolutions: device information, including but not limited to software in-ventory, audit logs (non-persistent) domain, email address, persona (if con-figured by the solutions admin). 		<p>por todos os serviços DEX, incluindo, entre outros, dados de desempenho do dispositivo , dados de desempenho do SO , dados de desempenho e instalação de software e dados de rede.</p> <p>- Dados pessoais processados em conexão com a sua utilização de módulos específicos:</p> <ul style="list-style-type: none"> • Análise da experiência: Dados de utilização, como dados de interação com o dispositivo , dados de interação com o navegador e respostas a pesquisas com usuário . • Gestão da experiência do aplicativo: Dados de software, como editor e versão do software, dados de interação com o software, dados de falhas e travamentos do software. • Experiência de Área de Trabalho Virtual: Dados da infraestrutura de desktop virtual, incluindo os registros de início e término da conexão . • Inteligência 1E: Dados pessoais, incluindo metadados de instruções e autor. • Informações sobre a atualização: patches ausentes e aplicados. • Serviços de integração: Por exemplo, informações do dispositivo , nomes de usuário. • Soluções SaaS: Informações do dispositivo , incluindo, entre outras, o software instalado. Inventário, registros de auditoria (não persistentes), domínio, endereço de e-mail, perfil (se configurado pelo administrador da solução).
--	--	--	--

ENGLISH

PORTUGUÊS

5 Categories of data subjects

The following categories of data subjects are affected by the data processing:

5 Categorias de titulares de dados

As seguintes categorias de titulares de dados são afetadas pelo processamento de dados:

Product	Nature and Purpose of the Processing	Produto	Natureza e propósito do processamento
<p>All TeamViewer products</p> <p>(e) except n- Engage/Co-Browsing function module, Classroom, see below)</p>	<ul style="list-style-type: none"> - Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - The connection partners of Customer/Customer's users. - Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by Customer/Customer's users. 	<p>Todos os produtos TeamViewer (exceto Engage/Co-Browsing, Sala de aula (ver abaixo))</p>	<ul style="list-style-type: none"> - Cliente (na medida em que os dados pessoais do Cliente sejam processados em de acordo com a seção 4) e, se aplicável, os usuários do Cliente, incluindo os usuários finais dos dispositivos gerenciados. - Parceiros de conexão do Cliente/Usuários do Cliente. - Terceiros gerenciados pelo Cliente/usuários do Cliente ou terceiros cujos dados pessoais são transmitidos pelo Cliente/usuários do Cliente.
<p>Engage/Co-Browsing function module</p> <p><Classroom></p>	<ul style="list-style-type: none"> - Users (Customer's customers, website visitors, prospects, third parties). - Customer's Employees (Agents). 	<p>Módulo de função de interação/navegação conjunta</p> <p>/Sala de aula</p>	<ul style="list-style-type: none"> - Usuários (clientes do cliente, visitantes do website, potenciais clientes, terceiros). - Funcionários do cliente (agentes).
<p>AI services</p>	<ul style="list-style-type: none"> - Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - The connection partners of Customer/Customer's users. Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by Customer/Customer's users 	<p>Serviços de IA</p>	<ul style="list-style-type: none"> - Cliente (na medida em que os dados pessoais do Cliente sejam processados em de acordo com a seção 4) e, se aplicável, os usuários do Cliente, incluindo os usuários finais dos dispositivos gerenciados. - Parceiros de conexão do Cliente/Usuários do Cliente. - Terceiros gerenciados pelo Cliente/usuários do Cliente, ou terceiros cujos dados pessoais são repassados pelo Cliente/usuários do Cliente
<p>DEX Services</p>	<ul style="list-style-type: none"> - Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by 	<p>Serviços DEX</p>	<ul style="list-style-type: none"> - Cliente (na medida em que os dados pessoais do Cliente sejam processados de acordo com a seção 4) e, se aplicável, usuários do Cliente, incluindo usuários finais de dispositivos gerenciados. - Terceiros gerenciados pelo Cliente/usuários do Cliente, ou terceiros cujos dados pessoais

	Customer/Customer's users.		são repassados pelo Cliente/usuários do Cliente.
--	----------------------------	--	--

ENGLISH

PORTUGUÊS

Appendix - Engage/Co-Browsing to Exhibit 1

Apêndice - Engajar/Navegação conjunta ao Anexo 1

1. Local Storage as website integration

1. Integração de armazenamento local com website.

Key	Related Feature/ Plugin	Purpose/Description	<Lifespan>	Chave	Recurso/Plugin relacionado	Finalidade/Descrição	Vida útil
cvvid	/	Msiteor-Id - can be assigned temporarily or permanently	Session or permanent	cvvid	/	Msiteor-Id - pode ser atribuído temporariamente ou permanentemente	Sessão ou permanente
Resume_i	Live Chat	"true" if privacy policy has been accepted in chat.	Session	CV_i	Chat ao vivo	"Verdadeiro" se a política de privacidade foi aceita no chat.	Sessão
résumé	Live Chat	Indicator whether a message has been sent or an interaction (e.g., button click) has taken place by The User.	Session	cv_sp	Chat ao vivo	Indicador que mostra se uma mensagem foi enviada ou se uma interação (por exemplo, clique em um botão) ocorreu. O Usuário.	Sessão
visited	Live Chat	"true" as soon as the User interacts with the Web-Chat for the first time - e.g., to trigger a chatbot only once.	Session	visitado	Chat ao vivo	"Verdadeiro" assim que o Usuário interage com o Web-Chat pela primeira vez - por exemplo, para acionar um chatbot. Apenas uma vez.	Sessão
cvssid	Co-Browsing	SessionId to ensure the continuity of a co-browsing session when changing pages or across multiple abs.	Session	cvsid	Navegação conjunta	SessionId para garantir a continuidade de uma sessão de co-navegação ao trocar de páginas ou entre várias sessões. □abs.	Sessão
résumé-shrid	Co-Browsing	5-digit numerical code through which an employee can connect to an employee by co-browsing.	Session	cv-shrid	Navegação conjunta	Código numérico de 5 dígitos através do qual um funcionário pode se conectar a outro funcionário por meio de co-navegação.	Sessão
Résumé-S	Co-Browsing	"true" as soon as customer releases his session or has requested co-browsing.	Session	CV-S	Navegação conjunta	"verdadeiro" assim que o cliente encerrar sua sessão ou solicitar a co-navegação.	Sessão
résumé-lvcs	Co-Browsing	Indicator that the session has been	Session	cv-lvcs	Navegação conjunta	Indicador de que a sessão foi encerrada	Sessão

		closed - necessary to end the co-browsing session across multiple open tabs.				- necessário para finalizar a sessão de co-navegação em várias plataformas. abas abertas da torta.	
CV_LVD	Co-Browsing	Temporary data for switching between two tabs - To ensure continuity of co-browsing session	Session	CV_LVD	Navegação conjunta	Dados temporários para alternar entre duas abas - Para garantir a continuidade da sessão de co-navegação.	Sessão

ENGLISH

PORTUGUÊS

2. Cookies for website integration

In order to enable continuous sessions not only on the same domain (e.g., user switches from yourweb-site.com to yourwebsite.com/imprint) but also across various Customer domains (e.g., user switches from yourwebsite.com to wiki.yourwebsite.com), the local storage variables are "converted" into cookies. In this case the purpose and naming remain the same as for the Local Storage Variables.

1. Cookies para integração do website

Para permitir sessões contínuas não apenas no mesmo domínio (por exemplo, quando o usuário alterna de yourweb-site.com para yourwebsite.com/imprint), mas também em vários domínios do cliente (por exemplo, quando o usuário alterna de yourwebsite.com para wiki.yourwebsite.com), as variáveis de armazenamento local são " " em cookies. Nesse caso, a finalidade e a nomenclatura permanecem as mesmas das variáveis de armazenamento local.

Key	Related Feature/ Plugin	Purpose/Description	<Lifespan>	Chave	Recurso/Plugin relacionado	Finalidade/Descrição	Vida útil
cvssid	Co-Browsing	Session-Id to ensure the continuity of a Co-Browsing session when changing pages or across multi-pie tabs.	Session	cvssid	Navegação conjunta	O ID da sessão garante a continuidade de uma sessão de co-navegação ao trocar de páginas ou entre várias abas do menu circular.	Sessão
résumé-shrid	Co-Browsing	5-digit numerical code through which an employee can connect to an employee by Co-Browsing.	Session	cv-shrid	Navegação conjunta	Código numérico de 5 dígitos através do qual um funcionário pode se conectar a outro funcionário por meio da navegação conjunta.	Sessão
Résumé-S	Co-Browsing	"true" as soon as customer releases his session or has requested Co-Browsing.	Session	CV-S	Navegação conjunta	"Verdadeiro" assim que o cliente encerrar a sessão ou solicitar a navegação conjunta.	Sessão
résumé-lvcs	Co-Browsing	Indicator that the session has been closed - necessary to end the Co-Browsing session across multiple open tabs.	Session	cv-lvcs	Navegação conjunta	Indicador de que a sessão foi encerrada - necessário para finalizar a sessão de Co-Navegação em várias plataformas. abas abertas da torta.	Sessão
CV_LVD	Co-Browsing	Temporary data for switching between two tabs - To ensure continuity of	Session	CV_LVD	Navegação conjunta	Dados temporários para alternar entre duas abas - Para garantir a continuidade da	Sessão

		Co-Browsing session.				sessão de co-navegação.	
--	--	----------------------	--	--	--	-------------------------	--

ENGLISH

PORTUGUÊS

3. Local storage for video chat and video consultations

3. Armazenamento local para videochamadas e consultas por vídeo.

Key	Related Feature/ Plugin	Purpose/Description	<Lifespan>	Chave	Funcionalidade/ Plugin relacionado	Finalidade/ Descrição	Vida útil
jitsiMeetId	Video Chat& Video Consultation	Unique ID for Video Chat session	Session	jitsiMeetId	Bate-papo por vídeo e consulta por vídeo - h:ion	ID exclusivo para sessão de videochamada	Sessão
language	Video Chat& Video Consultation	Specifies and maintains language of user interface	Session	linguagem	Bate-papo por vídeo e consulta por vídeo - h:ion	Especifica e mantém o idioma da interface do usuário .	Sessão
features/base /settings	Video Chat& Video Consultation	Technical variable	Session	características/ base /configurações	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
features/base /known-domains	Video Chat& Video Consultation	Technical variable	Session	características/ base /do-conhecido-domains	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
features/ drop-box	Video Chat& Video Consultation	Technical variable	Session	recursos/ caixa de seleção	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
features/ calendar-sync	Video Chat& Video Consultation	Technical variable	Session	recursos/ sincronização de calendário	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
features/recent/list	Video Chat& Video Consultation	Technical variable	Session	recursos/ recente/lista	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
features/video-layout	Video Chat& Video Consultation	Technical variable	Session	recursos/ layout de vídeo	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão

call-StatsUser Name	Video Chat& Video Consulta-h:ion	Technical variable	Session	nomeDeUsuário DeEstatísticas de chamada	Bate-papo por vídeo e consulta por vídeo - h:ion	Variável técnica	Sessão
cvvid	Video Chat& Video Consulta-h:ion	Visitor-ID - can be assigned temporarily or permanently	Session or permanent	cvvid	Bate-papo por vídeo e consulta por vídeo - h:ion	O ID do visitante pode ser atribuído temporariamente ou permanentemente.	Sessão ou permanente
CV_DOC_ID	Video Chat& Video Consulta-h:ion	Visitor-ID - for documents feature	Session	CV_DOC_UID	Bate-papo por vídeo e consulta por vídeo - h:ion	ID do visitante - recurso para documentos	Sessão
résumé	Video Chat& Video Consulta-h:ion	Tab-ID - defines on what tab in the video chat the user currently is (Video, Document, Whiteboard, Co-Browsing)	Session	cv-t	Bate-papo por vídeo e consulta por vídeo - h:ion	ID da aba - define em qual aba do bate-papo por vídeo o usuário está atualmente em (Vídeo, Documento, Quadro branco, Navegação conjunta)	Sessão
resume_sp	Video Chat& Video Consulta-h:ion	Indicator whether a message has been sent or an interaction (e.g., button click) has taken place by the user.	Session	cv_sp	Bate-papo por vídeo e consulta por vídeo - h:ion	Indicador que mostra se uma mensagem foi enviada ou não. A interação (por exemplo, clique em um botão) ocorreu por parte do Usuário.	Sessão

Appendix - Classroom to Annex 1 / Apêndice — Sala de Aula para o Anexo 1

ENGLISH

PORTUGUÊS

1. Local storage for video conference

1. Armazenamento local para videoconferências

Key	Related Feature/ Plugin	Purpose/Description	Lifespan	Chave	Funcionalidades relacionadas / Plugin	Proposito / Descrição	Vida útil
jitsiMeetId	Video Conference	Unique ID for Video Conference session	Session	jitsiMeetId	Videoconferência	ID exclusivo para sessão de videoconferência	Sessão
language	Video Conference	Specifies and maintains language of user interface	Session	linguagem	Videoconferência	Especifica e mantém o idioma da interface do usuário . face	Sessão
features/base /settings	Video Conference	Technical variable	Session	características/ base	Videoconferência	Variável técnica	Sessão

				/configurações			
features/base /known-domains	Video Conference	Technical variable	Session	características/ base / domínios-conhecidos	Videoconferência	Variável técnica	Sessão
features/drop-box	Video Conference	Technical variable	Session	recursos/ caixa de seleção	Videoconferência	Variável técnica	Sessão
features/calendar-sync	Video Conference	Technical variable	Session	recursos/ sincronização de calendário	Videoconferência	Variável técnica	Sessão
features/re-center/list	Video Conference	Technical variable	Session	recursos/ recente/ lista	Videoconferência	Variável técnica	Sessão
Features /video-layout	Video Conference	Technical variable	Session	Características / layout-de-vídeo	Videoconferência	Variável técnica	Sessão
call-StatsUserName	Video Conference	Technical variable	Session	chamar- Nome de usuário de estatísticas	Videoconferência	Variável técnica	Sessão
cvvid	Video Conference	Visitor-ID - can be assigned temporarily or permanently	Session or permanent	cvvid	Videoconferência	O ID do visitante pode ser atribuído temporariamente ou permanentemente.	Sessão ou permanente
CV_DOC_ID	Video Conference	Visitor-ID - for documents feature	Session	CV_DOC_UID	Videoconferência	ID do visitante - recurso para documentos	Sessão
résumé	Video Conference	Tab-ID - defines on what tab in the video chat the user currently is (Video, Document, Whiteboard)	Session	cv-t	Videoconferência	ID da aba - define em qual aba do bate-papo por vídeo o usuário está atualmente em (Vídeo, Documento, Quadro branco)	Sessão
resume_sp	Video Conference	Indicator whether a message has been sent or an interaction (e.g., button click) has taken place by the user.	Session	cv_sp	Videoconferência	Indicador que mostra se uma mensagem foi enviada ou se ocorreu uma interação do Usuário(por exemplo, um clique em um botão).	Sessão

ENGLISH

**Overview of Technical and
Organizational Measures**

PORTUGUÊS

**Visão Geral das Medidas Técnicas e
Organizacionais**

Content / Conteúdo

1	Access Control 2 / Controle de acesso	2
1.1	Data Centers	2
1.2	TeamViewer Offices 3 / Escritórios TeamViewer	3
2	System Access and Access Control 3 / Acesso ao Sistema e Controle de Acesso	3
2.1	Network and Hardware Security / Segurança de Rede e Hardware	3
2.2	Hiring ("Onboarding") and Departure ("Offboarding") of Employees 4 / Contratação ("Onboarding") e Desligamento ("Offboarding") de Funcionários	4
2.3	Data Access Control 4 / Controle de Acesso a Dados	4
2.4	Data Separation 4 / Separação de Dados	4
2.5	Pseudonymization / Pseudonimização	4
3	Measures to Establish the Integrity / Medidas para Estabelecer a Integridade	4
3.1	Transfer Control 4 / Controle de Transferência	4
3.2	Data Input Control / Controle de Entrada de Dados	5
4	Data Availability and Resilience of the Systems / Disponibilidade de Dados e Resiliência dos Sistemas	5
4.1	Incident Response Management 6 / Gestão de Resposta a Incidentes	6
5	Data Privacy Management / Gestão da Privacidade de Dados	6
5.1	Subprocessors / Subprocessadores	6
6	Data Protection by Design and by Default / Proteção de Dados desde a Concepção e por Padrão	6

ENGLISH

PORTUGUÊS

1 Access Control

1 Controle de Acesso

1.1 Data Centers

1.1 Centros de dados

TeamViewer does not own, lease or operate any TeamViewer server infrastructure for its offices or production environment. The TeamViewer corporate environment is a purely cloud-based infrastructure hosted in data centers provided by third parties. All third parties are certified under ISO 27001 standard.

A TeamViewer não possui, aluga ou opera nenhuma infraestrutura de servidores TeamViewer para seus escritórios ou ambiente de produção. O ambiente corporativo da TeamViewer é uma infraestrutura totalmente baseada em nuvem, hospedada em data centers fornecidos por terceiros. Todos os terceiros são certificados pela norma ISO 27001.

TeamViewer has access control measures in place to prevent unauthorized access to data processing equipment where personal data is stored or processed.

O TeamViewer possui medidas de Controle de Acesso para impedir o acesso não autorizado a equipamentos de processamento de dados onde dados pessoais são armazenados ou processados.

1.2 TeamViewer Offices

1.2 Escritórios TeamViewer

Only authorized persons have physical access to premises, buildings or rooms where the personal data is processed. TeamViewer facilities are protected by key systems, intrusion detection systems, access control measures and active key management. Access rights are granted to authorized staff on an individual basis, including visitors who must be accompanied by authorized personnel. Employees and visitors are required to wear their badges visibly at all times when on the premises.

Somente pessoas autorizadas têm acesso físico às instalações, edifícios ou salas onde os dados pessoais são processados. As instalações do TeamViewer são protegidas por sistemas de chaves, sistemas de detecção de intrusão, medidas de Controle de Acesso e gerenciamento ativo de chaves. Os direitos de acesso são concedidos a funcionários autorizados individualmente, incluindo visitantes que devem estar acompanhados por pessoal autorizado. Funcionários e visitantes são obrigados a usar seus crachás de forma visível o tempo todo quando estiverem nas instalações.

2 System Access and Access Control

2 Acesso ao sistema e Controle de Acesso

TeamViewer relies on the following system access control measures to prevent unauthorized persons from using data processing systems where personal data is stored or processed.

O TeamViewer utiliza as seguintes medidas de Controle de Acesso ao sistema para impedir que pessoas não autorizadas usem sistemas de processamento de dados onde dados pessoais são armazenados ou processados.

2.1 Network and Hardware Security

2.1 Segurança de rede e hardware

The TeamViewer corporate network is protected from the public network by firewalls and threat detection as well as subsequent removal systems. The latest anti-virus/malware detection software is used to detect, remove and prevent malicious code. Security patch management is implemented and remote access to the TeamViewer corporate network is protected by strong authentication mechanisms and a Virtual Private Network (VPN).

A rede corporativa da TeamViewer é protegida da rede pública por firewalls e sistemas de detecção e remoção de ameaças. O software de detecção / malware mais recente é usado para detectar, remover e prevenir códigos maliciosos. O gerenciamento de patches de segurança está implementado e o acesso remoto à rede corporativa da TeamViewer é protegido por mecanismos de autenticação robustos e uma Rede Virtual Privada (VPN).

TeamViewer uses a role-based security architecture and requires that users of the system be identified and authenticated before they can

O TeamViewer utiliza uma arquitetura de segurança baseada em funções e exige que os usuários do sistema sejam identificados e

use system resources. Resources are protected by native security and add-on software products that identify and authenticate users and validate access requests against users' authorized roles in access control lists.

All resources are managed in the asset inventory system and each resource is assigned an owner. The owners are responsible for approving access to the resource and performing checks on access by role.

Employees log in to the TeamViewer network with an Active Directory user ID and password. Users must also log in separately to any systems or applications that do not use Active Directory's split sign-on functionality. Passwords must meet defined password standards and are enforced by parameter settings in Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval. User IDs are locked after a certain number of unsuccessful login attempts to prevent access to system and resources. Additionally, after a defined period of inactivity, users' screens are locked automatically.

TeamViewer has a password policy that governs the proper use and setup of passwords, including the frequency with which they must be changed, minimum requirements, and complexity.

Employees accessing the system from outside, the TeamViewer network must use a VPN tunnel and two-factor authentication system. Employees are issued VPN certificates when they are hired, and access is disabled when they leave.

TeamViewer employees access the two-factor authentication services over the Internet by using the Secure Socket Layer (SSL) functionality of their web browser. The employees first enter a valid user ID and password to gain access to TeamViewer cloud resources. The passwords must match the password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured according to TeamViewer configuration defaults, but these configuration parameters can be changed using the virtual server administration account.

TeamViewer maintains a Security Operations Center (SOC) that monitors critical systems and alerts around the clock to manage security incidents. These services are operated in a compliant and data protection-friendly manner while ensuring a threat response that is appropriate to the organization's risk level.

TeamViewer employees can log in to their systems via virtual server administration accounts. These administration accounts use a two-tier authentication system based on digital certificates.

User IDs and access rules are defined according to

autenticados antes de poderem usar os recursos do sistema. Recursos são protegidos por segurança nativa e softwares add-on que identificam e autenticam os usuários e validam as solicitações de acesso de acordo com as funções autorizadas dos usuários nas listas de Controle de Acesso .

Os recursos são gerenciados no sistema de inventário de ativos e cada recurso tem um responsável atribuído. Os responsáveis são encarregados de aprovar o acesso ao recurso e verificar o acesso de acordo com a função.

Funcionários fazem login na rede TeamViewer com um ID de usuário e senha do Active Directory. Os usuários também devem fazer login separadamente em quaisquer sistemas ou aplicativos que não utilizem a funcionalidade de login dividido do Active Directory. As devem atender aos padrões de senha definidos e são aplicadas por meio de configurações Parâmetros no Active Directory. Essas configurações fazem parte dos padrões de configuração e Os usuários a alterar suas senhas em intervalos definidos. Os IDs de Usuário são bloqueados após um determinado número de tentativas de login malsucedidas para impedir o acesso ao sistema e aos recursos. Disso, após um período definido de inatividade, as telas dos usuários são bloqueadas automaticamente.

O TeamViewer tem uma política de senha que rege o uso e a configuração adequados de senhas, incluindo a frequência com que devem ser alteradas, os requisitos mínimos e a complexidade.

Que acessam o sistema de fora da empresa devem usar um túnel VPN e um sistema de autenticação de dois fatores na rede TeamViewer. Os certificados VPN são emitidos para os funcionários na contratação e o acesso é desativado quando eles se desligam da empresa.

Funcionários da TeamViewer acessam os serviços de autenticação de dois fatores pela Internet usando a funcionalidade Secure Socket Layer (SSL) do navegador. Primeiro, os funcionários inserem um ID de usuário e uma senha válidos para acessar os recursos da nuvem da TeamViewer. As devem corresponder aos requisitos de configuração de senha definidos nos dispositivos virtuais usando a conta de administração do servidor virtual. Os dispositivos São inicialmente configurados de acordo com as configurações padrão da TeamViewer, mas esses parâmetros podem ser alterados usando a conta de administração do servidor virtual.

TeamViewer mantém um Centro de Operações de Segurança (SOC) que monitora sistemas críticos e envia alertas 24 horas por dia, 7 dias por semana, para gerenciar incidentes de segurança. Esses serviços são operados de forma compatível com as normas e respeitando a proteção de dados, garantindo uma resposta a ameaças adequada ao nível de risco da organização.

Funcionários da TeamViewer podem acessar seus sistemas por meio de contas de administração de servidor virtual. Essas contas de administração usam um sistema de autenticação de dois níveis baseado em certificados digitais.

Os IDs de Usuário e as regras de acesso são

the role of each employee. Access rules are predefined based on the defined roles. When changes are made to a position, the associated rights and access rules are changed accordingly.

Regularly, access rights are reviewed by technical owners on the basis of team needs, tasks to be separated, and risks associated with access rights.

The revocation of rights and access as well as the deactivation of the account in the event of an employee's departure ("offboarding") or in the event of a change of position is carried out by the IT Service Desk to delete the employee's access or adjust the access rights.

Reporting Line Managers review the lists and enter the required changes into the event management record. The record is returned to the security help desk for processing. The IT Service Desk Manager identifies any records that have not been returned within two weeks and contacts the manager.

Only authorized persons can access systems that process personal data. TeamViewer uses multiple authorization levels when granting access to systems. All employees access TeamViewer's corporate systems via a personalized account (user ID) and have access only to the systems they need to access to perform their duties. Authorizations and privileges are reviewed on a regular basis. Similarly, rights to access systems are reviewed when the employees are assigned new roles or leave TeamViewer.

2.2 Hiring ("Onboarding") and Departure ("Offboarding") of Employees

When an employee is hired, they are assigned to a position in the HR management system. Before the employee's start date, the HR team creates a so-called "onboarding" ticket that contains the employee's user IDs and the access rights to be granted. The ticket is used by the IT service desk to create user IDs and access rules. The access rules are defined according to the minimal principle (each employee is granted only the permissions he/she needs to perform his/her task). In addition, the ticket system contains a template for employees who change their position and the associated rights, which must be changed accordingly within the existing access rules.

Access rights of technical owners are reviewed regularly to determine if they need to be revoked. When evaluating access rights, team leaders consider the job description, the tasks to be separated, and the risks associated with access rights.

definidos de acordo com a função de cada funcionário. As regras de acesso são predefinidas com base nas funções definidas. Quando há alterações em um cargo, os direitos e as regras de acesso associados são alterados de acordo.

Regularmente, os direitos de acesso são revisados pelos responsáveis técnicos com base nas necessidades da equipe, nas tarefas a serem separadas e nos riscos associados aos direitos de acesso.

A revogação de direitos e acessos, bem como a desativação da conta em caso de desligamento do funcionário ("offboarding") ou em caso de mudança de cargo, é realizada pela Central de Serviços de TI para excluir o acesso do funcionário ou ajustar os direitos de acesso.

Os gerentes de linha de reporte revisam as listas e inserem as alterações necessárias no registro de gerenciamento de eventos. O registro é devolvido à central de atendimento de segurança para processamento. O gerente da central de atendimento de TI identifica quaisquer registros que não tenham sido devolvidos em até duas semanas e entra em contato com o gerente.

Somente pessoas autorizadas podem acessar sistemas que processam dados pessoais. O TeamViewer usa vários níveis de autorização ao conceder acesso aos sistemas. Todos os funcionários acessam os sistemas corporativos do TeamViewer por meio de uma conta personalizada (ID de usuário) e têm acesso somente aos sistemas necessários para o desempenho de suas funções. As autorizações e os privilégios são revisados regularmente. Da mesma forma, os direitos de acesso aos sistemas são revisados quando os funcionários recebem novas funções ou deixam o TeamViewer.

2.2 Contratação ("Onboarding") e desligamento ("Offboarding") de funcionários

Quando um funcionário é contratado, ele é alocado a um cargo no sistema de gestão de RH. Antes da data de início do funcionário, a equipe de RH cria um chamado "ticket de integração" que contém os IDs de usuário do funcionário e os direitos de acesso a serem concedidos. O ticket é usado pela central de atendimento de TI para criar IDs de usuário e regras de acesso. As regras de acesso são definidas de acordo com o princípio do minimalismo (cada funcionário recebe apenas as permissões necessárias para desempenhar sua função). Além disso, o sistema de tickets contém um modelo para funcionários que mudam de cargo e os direitos associados, que devem ser alterados de acordo com as regras de acesso existentes.

Os direitos de acesso dos responsáveis técnicos são revisados regularmente para determinar se precisam ser revogados. Ao avaliar os direitos de acesso, os líderes de equipe consideram a descrição do cargo, as tarefas a serem separadas e os riscos associados aos direitos de acesso.

After an employee's employment ends, the HR department creates an offboarding ticket. These tickets are processed automatically to remove the employee's access in all systems. The IT Service Desk uses the tickets to lock user IDs and delete all access roles from IDs owned by the ticket's employee. TeamViewer will carry out regular checks into these lists to ensure that automated corrections have been implemented correctly.

O término do contrato de trabalho de um funcionário, o departamento de RH cria um chamado de desligamento. Esses São processados automaticamente para remover o acesso do funcionário a todos os sistemas. A Central de Serviços de TI usa os Para bloquear IDs de usuário e excluir todas as funções de acesso dos IDs pertencentes ao funcionário do chamado. O TeamViewer realiza verificações regulares nessas listas para garantir que as correções automáticas tenham sido implementadas corretamente.

2.3 Data Access Control

TeamViewer controls access to systems containing personal data through a mixture of role-based access control (RBAC) and user rights management. This ensures that access to and use of data is minimized, both in terms of general processing and in terms of the list and scope of access for TeamViewer employees. These access controls vary depending on the sensitivity of the data stored and operational requirements. In addition to granting access to individual employees, for some systems, specific access can be granted for a limited amount of time with an approval process. Also, workload identity federation is being used to grant access to resource on specific systems.

2.3 Controle de Acesso a dados

TeamViewer controla o acesso a sistemas que contêm dados pessoais por meio de uma combinação de Controle de Acesso baseado em funções (RBAC) e gerenciamento de direitos de usuário. Isso garante que o acesso e o uso dos dados sejam minimizados, em termos de processamento geral quanto em termos da lista e do escopo de acesso para os funcionários do TeamViewer. Esses controles de acesso variam dependendo da sensibilidade dos dados armazenados e dos requisitos operacionais. Além de conceder acesso a funcionários individuais, para alguns sistemas, o acesso específico pode ser concedido por um período limitado de tempo com um processo de aprovação. A federação de identidade de carga de trabalho está sendo usada para conceder acesso a recursos em sistemas específicos.

2.4 Data Segregation

The networks are segregated and segmented. This works within RBAC to minimize risks in line with sound security and data protection practices. For example, data for different products/purposes are processed separately where possible, including by separating production and test environments. Where appropriate, data is processed separately to avoid unnecessary mixing of data and processing beyond the purpose.

2.4 Separação de dados

As redes são segregadas e segmentadas. Isso funciona dentro do RBAC para minimizar riscos, em conformidade com boas práticas de segurança e proteção de dados. Por exemplo, dados para diferentes produtos/finalidades são processados separadamente sempre que possível, inclusive separando ambientes de produção e teste. Quando apropriado, os dados são processados separadamente para evitar a mistura desnecessária de dados e o processamento além da finalidade.

2.5 Pseudonymization

TeamViewer uses pseudonymization where it can be applied without affecting the efficiency of processes and/or where it is necessary to protect data in the event that disclosure is required. Where possible as part of the disclosure process, anonymization is used. Data that can identify data subjects contained in pseudonymized data is stored separately and encrypted where possible.

TeamViewer has a process for assessing internal data sharing and uses pseudonymization to limit the use of personal data for certain purposes.

2.5 Pseudonimização

O TeamViewer utiliza pseudonimização sempre que possível, sem afetar a eficiência dos processos e/ou quando necessário para proteger os dados em caso de divulgação. Que possível, a anonimização é utilizada como parte do processo de divulgação. Os dados que podem identificar Titulares dos dados contidos em dados pseudonimizados são armazenados separadamente e criptografados sempre que possível.

O TeamViewer tem um processo para avaliar o compartilhamento interno de dados e usa pseudonimização para limitar o uso de dados pessoais a determinados fins.

3 Measures to Establish the Integrity

3.1 Transfer Control

TeamViewer has transfer controls in place to ensure that data is secure during transmission and that the level of protection does not fall below a minimum standard once it leaves the perimeter.

These security measures include securing transmissions with SSL/TLS, https, etc. and the use of VPNs throughout the organization. TeamViewer maintains firewalls and other standard security systems to protect its operations and data.

Firewall systems are in place to filter unauthorized incoming network traffic from the Internet and to deny any type of network connection that is not explicitly authorized.

3.2 Data Input Control

TeamViewer has systems in place to log who has accessed or modified personal data, including linking such controls to individual accounts.

4 Data Availability and Resilience of the Systems

TeamViewer creates backups of critical data in accordance with common practice and ensures that these backups act as a reliable failover in the event of a catastrophic failure.

Customer data is backed up and monitored by Operations staff for completeness and disruptions. In the event of a disruption, the Operations staff performs troubleshooting to identify the root cause and then reruns the backup job immediately or as part of the next scheduled backup job. Backup infrastructure is physically secured in locked cabinets and/or caged environments within third-party data center. The backup infrastructure resides on private networks that are logically secured from other networks.

Incident response policies and procedures are in place to guide the personnel in reporting and dealing with information technology incidents. Procedures are in place to detect, report, and respond to system security breaches and other incidents. Incident response procedures are in place to detect and respond to incidents on the network.

TeamViewer monitors the utilization of physical and computer infrastructure, both internally and for customers, to ensure that service delivery meets service level agreements.

3 Medidas para estabelecer a integridade

3.1 Controle de transferência

O TeamViewer possui controles de transferência para garantir que os dados estejam seguros durante a transmissão e que o nível de proteção não caia abaixo de um padrão mínimo assim que saírem do perímetro.

De segurança incluem a proteção das transmissões com SSL/TLS, https, etc., e o uso de VPNs em toda a empresa. A TeamViewer mantém firewalls e outros sistemas de segurança padrão para proteger suas operações e dados.

Os sistemas de firewall existem para filtrar o tráfego de rede não autorizado vindo da Internet e para negar qualquer tipo de conexão de rede que não seja explicitamente autorizada.

3.2 Controle de entrada de dados

O TeamViewer possui sistemas para registrar quem acessou ou modificou dados pessoais, incluindo a vinculação desses controles a contas individuais.

4 Disponibilidade de dados e resiliência dos sistemas

O TeamViewer cria backups de dados críticos de acordo com as práticas comuns e garante que esses backups atuem como uma alternativa confiável em caso de falha catastrófica.

Os dados dos clientes são copiados e monitorados pela equipe de Operações para garantir integridade e detectar interrupções. Em caso de interrupção, a equipe de Operações realiza a solução de problemas para identificar a causa raiz e, em seguida, executa o backup novamente imediatamente ou como parte do próximo backup agendado. A infraestrutura de Backup é fisicamente protegida em gabinetes trancados e/ou ambientes isolados dentro de um data center de terceiros. A infraestrutura de backup reside em redes privadas que são logicamente protegidas de outras redes.

As políticas e os procedimentos de resposta a incidentes estão em vigor para orientar a equipe na comunicação e no tratamento de incidentes de tecnologia da informação. Os procedimentos estão em vigor para detectar, relatar e responder a violações de segurança do sistema e outros incidentes. Os procedimentos de resposta a incidentes estão em vigor para detectar e responder a incidentes na rede.

O TeamViewer monitora a utilização da infraestrutura física e de dispositivo, tanto interna quanto para clientes, para garantir que a prestação de serviços atenda aos acordos de nível de serviço.

TeamViewer evaluates the need for additional infrastructure capacity in response to the growth of existing customers or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Data center space, power, and cooling
- Disk storage
- Tape storage
- Network bandwidth

TeamViewer has implemented a patch management process to ensure that the customer relevant and infrastructure systems used for the service on the TeamViewer side are patched in accordance with operating system patches recommended by the respective vendor. TeamViewer system owners review proposed operating system patches to determine if the patches are applied.

TeamViewer is responsible for determining the risk of applying or not applying patches based on the security and availability impact of these systems and any critical applications hosted on them. TeamViewer staff will verify that all patches have been applied and that a restart has been performed, if applicable.

Redundancy is built into the system infrastructure that supports the data center services to ensure that there is no single point of failure, which includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is performed to measure the security posture of a target system or environment. The commissioned third-party vendor uses an industry-standard penetration testing methodology specified by TeamViewer. The third-party vendor's approach begins with a vulnerability assessment of the target system to determine what vulnerabilities exist on the system that can be exploited through a penetration test, simulating a disgruntled/affected insider or an attacker who has gained internal access to the network.

Once the vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine if unauthorized access or other malicious activity is possible.

Penetration testing includes testing of the network and application layers, as well as testing of the controls and processes around the networks and applications. Testing is performed both externally (external testing) and within the network.

Vulnerability scans are performed daily by TeamViewer in accordance with its internal policies. Upon request by a customer and at TeamViewer's discretion, a penetration test may also be performed by a third-party vendor in accordance with TeamViewer policies. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by TeamViewer. These technologies are customized to efficiently test the organization's infrastructure and software while minimizing the potential risks associated with active scanning.

Retests and on-demand scans are performed as needed. Vulnerability Scans are performed outside of peak business hours.

O TeamViewer avalia a necessidade de capacidade de infraestrutura adicional em resposta ao crescimento de clientes existentes ou à aquisição de novos clientes. O monitoramento da capacidade de infraestrutura do Includi, entre outros, os seguintes itens:

- Espaço, energia e refrigeração do data center
- Armazenamento em disco
- Armazenamento de fita
- Largura de banda da rede

O TeamViewer implementou um processo de gerenciamento de patches para garantir que os sistemas relevantes do cliente e a infraestrutura usada para o serviço no lado do TeamViewer estejam atualizados de acordo com os patches do sistema operacional recomendados pelo respectivo fornecedor. Os proprietários dos sistemas Revisam os patches de sistema operacional propostos para determinar se eles serão aplicados.

A TeamViewer é responsável por determinar o risco de aplicar ou não patches com base no impacto na segurança e disponibilidade desses E de quaisquer aplicativos críticos hospedados neles. A equipe da TeamViewer verificará se todos os patches foram aplicados e se a reinicialização foi realizada, se necessário.

Redundância é um recurso integrado à infraestrutura de sistemas que suporta os serviços do data center, garantindo que não haja um único ponto de falha. Isso inclui firewalls, roteadores e servidores. Se um sistema primário falhar, o hardware redundante é configurado para substituí-lo.

O teste de penetração é realizado para medir o nível de segurança de um sistema ou ambiente alvo. O fornecedor terceirizado contratado utiliza uma metodologia de teste de penetração padrão do setor, especificada pela TeamViewer. A abordagem do fornecedor terceirizado começa com uma avaliação de vulnerabilidades do sistema alvo para determinar quais vulnerabilidades existem no sistema que podem ser exploradas por meio de um teste de penetração, simulando um funcionário insatisfeito/afetado ou um invasor que obteve acesso interno à rede.

Depois que as vulnerabilidades são identificadas, o fornecedor terceirizado tenta explorá-las para determinar se é possível obter acesso não autorizado ou realizar outras atividades maliciosas.

Teste de penetração inclui testes nas camadas de rede e de aplicação, bem como testes nos controles e processos que envolvem as redes e aplicações. Os testes são realizados tanto externamente (testes externos) quanto dentro da rede.

TeamViewer realiza varreduras de vulnerabilidades diariamente De acordo com suas políticas internas. A pedido do cliente e a critério da TeamViewer, um teste de penetração também pode ser realizado por um fornecedor terceirizado, em conformidade com as políticas da TeamViewer. O fornecedor Utiliza tecnologias de varredura padrão do setor e uma metodologia formal especificada pela TeamViewer. Essas tecnologias são personalizadas para testar com eficiência a infraestrutura e o software da organização, minimizando os riscos potenciais associados à varredura ativa.

Retestes e as varreduras sob demanda são realizados conforme necessário. As varreduras de vulnerabilidades são realizadas fora do horário comercial de pico.

Tools that need to be installed in the TeamViewer system are implemented via the change management process. Scanning is performed with approved scan templates and with bandwidth throttling options enabled.

4.1 Incident Response Management

TeamViewer maintains contingency plans to respond to potential security threats. The incident response plan has defined processes to detect, mitigate, investigate, and report security incidents. It includes incident verification, attack analysis, containment, data collection, and problem remediation.

If TeamViewer becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data of Customer while processed by TeamViewer, TeamViewer will notify Customer of such a security incident, provide information about the security incident and take appropriate measures to mitigate adverse effects and to minimize any damage from the security incident, according to the stipulations in the Data Processing Agreement.

To be notified of recent security updates, a [security bulletin](#) is available for subscription.

Ferramentas que precisam ser instaladas no sistema TeamViewer são implementadas por meio do processo de gerenciamento de mudanças. A varredura é realizada com modelos de varredura aprovados e com opções de limitação de largura de banda ativadas.

4.1 Gestão de Resposta a Incidentes

O TeamViewer mantém planos de contingência para responder a possíveis ameaças à segurança. O plano de resposta a incidentes define processos para detectar, mitigar, investigar e relatar incidentes de segurança. Ele inclui verificação de incidentes, análise de ataques, contenção, coleta de dados e resolução de problemas.

Caso a TeamViewer tome conhecimento de uma violação de segurança que leve à destruição, perda, alteração, divulgação não autorizada ou acesso accidental ou ilegal aos dados pessoais do Cliente enquanto processados pela TeamViewer, a TeamViewer notificará o Cliente sobre tal incidente de segurança, fornecerá informações sobre o incidente e tomará as medidas apropriadas para mitigar os efeitos adversos e minimizar quaisquer danos decorrentes do incidente, de acordo com as estipulações do Adendo de Processamento de Dados (ADP).

Para ser notificado sobre as atualizações de segurança mais recentes, um boletim de segurança está disponível para assinatura.

5 Data Privacy Management

TeamViewer maintains comprehensive privacy policies and procedures for which the Data Protection Officer (DPO) and TeamViewer management are ultimately responsible. TeamViewer continually updates its privacy and security measures in accordance with updated policies, applicable laws and best practices. This includes regular reviews of documentation of procedures, training, and technical and organizational measures, maintaining and creating records of processing activities, and conducting data protection impact assessments, including other relevant assessments, as appropriate.

TeamViewer has processes, policies and procedures that describe physical security, logical access, computer operations, change control and data communication standards. All employees are obliged to adhere to TeamViewer policies and procedures that define how services are to be delivered. These are located on the company intranet and can be viewed by any TeamViewer employee.

The Employees receive regular data protection training and are bound to confidentiality. TeamViewer conducts regular awareness training for employees at least once a year, but the frequency may increase as needed.

5 Gestão da Proteção de Dados

TeamViewer mantém políticas e procedimentos de privacidade abrangentes, pelos quais o Encarregado de Proteção de Dados (DPO) e a administração da TeamViewer são os responsáveis finais. A TeamViewer atualiza continuamente suas medidas de privacidade e segurança de acordo com as políticas atualizadas, as leis e as melhores práticas. Isso inclui revisões regulares da documentação de procedimentos, treinamentos e medidas técnicas e organizacionais, manutenção e criação de registros de atividades de processamento e realização de avaliações de impacto sobre a proteção de dados, incluindo outras avaliações relevantes, conforme apropriado.

A TeamViewer possui processos, políticas e procedimentos que descrevem a segurança física, o acesso lógico, as operações de dispositivo, o controle de alterações e os padrões de comunicação de dados. Todos os funcionários são obrigados a seguir as políticas e os procedimentos da TeamViewer que definem como os serviços devem ser prestados. Esses documentos estão localizados na intranet da empresa e podem ser visualizados por qualquer funcionário da TeamViewer.

Funcionários recebem treinamento regular sobre proteção de dados e estão sujeitos à confidencialidade. A TeamViewer realiza treinamentos regulares de conscientização para os funcionários pelo menos uma vez por ano, mas a frequência pode aumentar conforme necessário.

TeamViewer designates at least one person per department who is responsible for compliance and implementation of the requirements of the General Data Protection Regulation (GDPR). All responsible data protection staff members have at least one IAPP CIPP qualification (or equivalent) relevant to their area of work.

A review of the effectiveness of the technical and organizational measures is carried out at least annually. Data protection impact assessments and other relevant assessments are carried out when necessary.

There is a formalized policy for handling data subject requests under the GDPR.

All employees are trained internally in accordance with Art. 32 (4) GDPR and are obligated to ensure that personal data is handled in accordance with data protection requirements.

After termination of the contractual relationship with the employee, the data will be deleted in accordance with the principles of data protection with data minimization taken into account.

5.1 Subprocessors

TeamViewer enters into a Data Processing Agreement (DPA) with all subprocessors of personal data. Furthermore, TeamViewer ensures that all subprocessors comply with the relevant security and data protection standards and that these requirements and obligations are included as part of the DPA. DPAs meet the requirements of the GDPR including (where applicable) the latest version of the Standard Contractual Clauses.

In the case of long-term cooperation, there is an ongoing review of subprocessors and the level of protection afforded to data processed with each one.

A TeamViewer designa pelo menos uma pessoa por departamento responsável pela conformidade e implementação dos requisitos do Regulamento Geral de Proteção de Dados (RGPD). Todos os membros da equipe responsáveis pela proteção de dados possuem pelo menos uma certificação IAPP CIPP (ou equivalente) relevante para sua área de atuação.

Uma avaliação da eficácia das medidas técnicas e organizacionais é realizada pelo menos anualmente. Avaliações de impacto sobre a proteção de dados e outras avaliações relevantes são realizadas quando necessário.

Existe uma política formalizada para lidar com solicitações de titulares de dados de acordo com o GDPR.

os funcionários são treinados internamente de acordo com o Art. 32 (4) do GDPR e são obrigados a garantir que os dados pessoais sejam tratados de acordo com os requisitos de proteção de dados.

Após o término do vínculo contratual com o funcionário, os dados serão apagados de acordo com os princípios de proteção de dados, levando-se em consideração a minimização dos mesmos.

5.1 Subprocessadores

TeamViewer celebra um Adendo de Processamento de Dados (ADP) (Adendo de Processamento de Dados (ADP)) com todos os subcontratados de dados pessoais. Além disso, a Garante que todos os subcontratados cumpram os padrões de segurança e proteção de dados relevantes e que esses requisitos e obrigações estejam incluídos no Adendo de Processamento de Dados (ADP). Os DPAs atendem aos requisitos do GDPR, incluindo (quando aplicável) a versão mais recente das Cláusulas Contratuais Padrão.

No caso de cooperação a longo prazo, há uma revisão contínua dos subcontratados e do nível de proteção oferecido aos dados processados por cada um deles.

6 Data Protection by Design and by Default

Personal data is collected and processed only to the extent necessary for the prescribed purpose. Data subjects have a simple way to exercise their rights.

Data protection principles are already observed during software development. In particular, the employees are encouraged and trained to implement technical and organizational measures as part of product development that ensure compliance with the requirements of GDPR and, specifically the rights of data subjects. The software is designed in such a way that the amount of data collected as well as the scope of processing is limited to the extent necessary. Insofar as various settings options exist within the software, the setting in which the smallest possible amount of personal data is processed is always selected in the delivery state, excluding core functionalities. Development teams work in close relation with the privacy team to ensure data protection requirements are implemented in TeamViewer's products.

6 Proteção de dados desde a concepção e por padrão

Os dados pessoais são coletados e processados apenas na medida necessária para a finalidade descrita. Os titulares dos dados têm uma maneira simples de exercer seus direitos.

Os princípios de proteção de dados já são observados durante o desenvolvimento de software. Em particular, os funcionários são incentivados e treinados para implementar medidas técnicas e organizacionais como parte do desenvolvimento do produto, garantindo a conformidade com os requisitos do GDPR e, especificamente, com os direitos dos titulares dos dados. O software é projetado de forma que a quantidade de dados coletados, bem como o escopo do processamento é limitado ao estritamente necessário. Na medida em que existam várias opções de configuração no software, a configuração que processa a menor quantidade possível de dados pessoais é sempre selecionada na configuração de entrega, excluindo as funcionalidades principais. De desenvolvimento trabalham em estreita colaboração com a equipe de privacidade para garantir que os requisitos de proteção de dados sejam implementados nos produtos TeamViewer.

With respect to change control, TeamViewer maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include as follows: Change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is used to document change control procedures for changes in the application and implementation of new changes.

Quality assurance tests and results are documented and maintained along with the corresponding change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents these approvals in the ticketing system. Version control software is used to manage source code versions and migrate source code through the development process to the production environment. Version control software maintains a history of code changes to support rollback capabilities and tracks changes for developers.

All infrastructure changes to the environment are reviewed and approved by the Change Advisory Board (CAB). The CAB consists of, at a minimum, the Head of the IT Infrastructure, the Head of the Application and Demand Management, a member of the IT Security Team, and the change requester. This ensures that all changes are reviewed, and that the quality of the implementation is maintained.

Com relação ao controle de mudanças, o TeamViewer mantém políticas e procedimentos documentados do Ciclo de Vida de Desenvolvimento de Software () para orientar a equipe na documentação e implementação de alterações em aplicativos e infraestrutura. Os procedimentos de controle de mudanças incluem: processos de solicitação e iniciação de mudanças, requisitos de documentação, práticas de desenvolvimento, requisitos de testes de garantia de qualidade e procedimentos de aprovação necessários.

Um sistema de tickets é usado para documentar os procedimentos de controle de mudanças para alterações no aplicativo e a implementação de novas mudanças.

Os testes e resultados de garantia de qualidade são documentados e mantidos juntamente com a respectiva solicitação de alteração. O desenvolvimento e os testes são realizados em um ambiente logicamente separado do ambiente de produção. A gerência aprova as alterações antes da migração para o ambiente de produção e documenta essas aprovações no sistema de tickets. Um software de controle de versão é usado para gerenciar as versões do código-fonte e migrá-lo durante o processo de desenvolvimento até o ambiente de produção. O software de controle de versão mantém um histórico das alterações de código para oferecer suporte a recursos de reversão e rastrear as alterações para os desenvolvedores.

Todas as alterações de infraestrutura no ambiente são revisadas e aprovadas pelo Conselho Consultivo de Mudanças (CAB). O CAB é composto, no mínimo, pelo Chefe de Infraestrutura de TI, o Chefe de Gerenciamento de Aplicativos e Demandas, um membro da Equipe de Segurança de TI e o solicitante da mudança. Isso garante que todas as mudanças sejam revisadas e que a qualidade da implementação seja mantida.

[Annex 3 to the Data Processing Agreement](#)
[Anexo 3 ao Acordo de Processamento de Dados](#)

Subprocessor List / Lista de Subprocessadores

Version as of March 9, 2026

ENGLISH

PORTUGUÊS

The following entities may process your personal data as subprocessor or further subprocessor, depending on your contractual partner.

As seguintes entidades podem processar os seus dados pessoais como subcontratadas ou subcontratadas adicionais, dependendo do seu parceiro contratual.

1. Subprocessors for TeamViewer's products {except Frontline, Engage/Co-Browsing, Classroom, see separate Sections below}

1. Subprocessadores para os produtos TeamViewer (exceto Frontline, Engage/Co-Browsing e Classroom; consulte as seções separadas abaixo)

Name	Location	Provided Service
Anexia Internetdienstleistungs GmbH	Feldkirchnerstrasse 140, 9020 Klagenfurt, Austria	Hosting
Amazon Web Services EMEA Sarl (except Assist AR)	38 Avenue John F. Kennedy, L-1855 Luxemburg	Hosting
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Ireland	Hosting
Schwarz Digits IT KG	Stiftsbergstraße 1, 74172 Neckarsulm, Germany	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Maintenance and Development
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Austria	Maintenance and Hosting
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Goepfingen, Germany	TeamViewer Products and Services

Additional Features, against separate order or activation of function modules		
Malwarebytes Inc. (<i>only applicable for the function modules Threatdown Endpoint Protection/Endpoint Detection & Response</i>)	3979 Freedom Circle, Santa Clara, CA 95054, USA	Threatdown Endpoint Protection; Endpoint Detection & Response (<i>optional</i>)
Lansweeper NV (<i>only applicable for the Asset Management and Discovery</i>)	Fraterstraat 212, 9820 Merelbeke, Belgium	Asset Management and Discovery (<i>optional</i>)
Ivanti UK Limited (<i>only applicable for the Mobile Device Management</i>)	3 Arlington Square Downshire Way, Bracknell, RG12 1WA, United Kingdom	Mobile Device Management (<i>optional</i>)
1ELimited	2nd Floor Midas House, 62 Goldsworth Road, Woking, Surrey, GU21 6LQ, United Kingdom	DEX services (<i>optional</i> , hosting locations as agreed)
Workato, Inc.	215 Castro St., Suite 300, Mountain View, CA 94041, USA	Automations (<i>optional</i> , EU hosting location)
Exclusively for connections from and to China		
Alibaba.com (Europe) Limited	Herengracht 448, 1017 CA, Amsterdam, the Netherlands	Hosting

2. Subprocessors for TeamViewer Frontline / Subprocesador para Frontline

Name	Location	Provided Service
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Maintenance and Development
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Ireland	Hosting

TeamViewer Germany GmbH	Bahnhofplatz 2, 73033 Goeppingen, Germany	TeamViewer Products and Services
Additional Features, on specific request or under special circumstances		
Twilio Inc. <i>(only if requested by the Customer)</i>	375 Beale Street, Suite 300, San Francisco, CA 94105, USA	Hosting of the video and audio feed <i>(optional)</i>
Business Objects Software Limited ("SAP") <i>(only applicable for the Customers using the SAP Global Partner Support Center)</i>	1012 - 1014 Kingswood Avenue, Citywest Business Campus, Dublin 24, Ireland	Hosting of customer support portal <i>(optional)</i>

3. Subprocessors for TeamViewer Engage/ Co-Browsing/ Classroom / Subprocessador para TeamViewer Engage / Co-Browsing / Classroom

Name	Location	Provided Service
Amazon Web Services EMEA LLC	38 Avenue John F. Kennedy, 1855 Luxembourg	Hosting
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany	Hosting
TeamViewer Greece LLC	Leoforos Dodonis 147 45221Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal LLC TeamViewer Austria LLC TeamViewer Germany LLC	Rua Manuel Pinto de Azevedo, 860, 7th, 4100-320 Porto, Portugal Graben 5, 4020 Linz, Austria Bahnhofspatz 2, 73033 Goeppingen, Germany	Maintenance and Development Maintenance and Hosting. Hosting locations for Engage/Co-Browsing: for all customers- EU; only for Japanese customers - Japan Hosting location for Classroom: EU TeamViewer Products and Services

4. Subprocessors for DEX services / Subprocessador para serviços DEX

Name	Location	Provided Service
Atlassian Pty Ltd.	350 Bush Street Floor 13 San Francisco, CA 94104 United States	Customer Support AI Services
Datadog Inc.	620 8th Ave 45th Floor, New York, NY 10018, United States	Monitoring and Logging
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
Outsystems Inc.	55 Thomson Place, 2nd floor, Boston MA 02210, United States	Development platform used to design and deploy DEX services
Pendo.io, Inc.	Raleigh, 301 Hillsborough St, Suite 1900, United States	1E Application UI
1E Limited	2nd Floor Midas House, 62 Goldsworth Road, Woking, Surrey, GU21 6LQ, United Kingdom	DEX services (hosting locations as agreed)
ThoughtSpot Inc.	444 Castro Street, Suite 1000 Mountain View, CA 94041, United States	Customizable Reporting
Project Hosts Inc.	201 N. Spence Ave. STE 101 Goldsboro, NC 27534, United States	Hosting (FedRAMP tenants only)

5. Professional Services and Support / Serviços profissionais e suporte

Name	Location	Provided Service
TeamViewer Affiliates	Affiliated Companies	Professional Services, Service Level Support, Customer Support