Contrato de Processamento de Dados (“DPA”) para os Serviços em Nuvem da Unify

Em vigor a partir de 15 de maio de 2018 (a “Data de Vigência”)

Firmado entre o Cliente (“Cliente” ou “Controlador”) e a Unify Software and Solutions GmbH & Co.KG (“Unify” ou “Co-Controlador”)

O Cliente e a Unify cada uma delas denominada como uma “Parte” e, coletivamente, as “Partes”.

Os Serviços em Nuvem da Unify permitem que o Cliente e seus usuários insiram informações para processamento através do software fornecido como um serviço - SaaS. Na medida em que estas informações contenham Dados Pessoais, as Partes concordam expressamente que este DPA se aplicará, no qual ambas as Partes compartilham as funções e responsabilidades de um Controlador da seguinte maneira:

- O Cliente (i) é responsável por definir os objetivos do Processamento de Dados Pessoais, (ii) é responsável pela exatidão dos Dados Pessoais, (iii) é responsável por informar os titulares dos dados sobre o processamento de Dados Pessoais e as modalidades para o exercício de seus direitos, e (iv) é responsável por elaborar notificações (incluindo notificações de violação de proteção de dados) às autoridades de proteção de dados, se necessário.
- A Unify (i) define os meios do Processamento e (ii) é responsável pela implementação das medidas de segurança,

e a Unify assume, além disso, a função de Processador de acordo com as definições na seção 1. Essas funções e responsabilidades são detalhadas na Seção 4 (Funções e Responsabilidades) abaixo.

Este DPA se aplica a todas as atividades realizadas pela Unify no âmbito dos Serviços em Nuvem da Unify e dos Termos de Produção de Serviços (TOSP) para esses Serviços em Nuvem da Unify https://unify.com/br/informacoes-legais/dps-para-circuit, por meio do qual os funcionários da Unify ou terceirizados subcontratados pela Unify podem processar os Dados Pessoais do Cliente.

O DPA não se aplica a nenhum outro produto, site ou serviço da Unify on-line ou off-line. Com relação aos Serviços em Nuvem da Unify, este DPA prevalece sobre qualquer outro contrato de processamento de dados existente ou acordo semelhante entre a Unify e o Cliente que possa estar em vigor para outros produtos, sites ou serviços.

O Cliente reconhece que recebeu todas as informações que considera necessárias para estabelecer o fato de que a Unify fornece garantias suficientes com relação à proteção dos Dados Pessoais.

1 Definições

Além dos termos definidos em outras partes do TOSP, as seguintes definições se aplicam:

- “Lei de proteção de dados aplicável”: significa as leis e regulamentos relacionados ao processamento e proteção de dados pessoais aplicáveis no país onde a Unify está estabelecida. Em especial, a Lei Aplicável significa (a) Lei de Proteção de Dados Pessoais (LGPD ou Lei 13.709/18) e Regulamento UE 2016/679 (Regulamento Geral de Proteção de Dados; 'GDPR') (b) Leis ou regulamentos dos Estados Membros relacionados ao processamento e proteção de Dados Pessoais que implementam ou complementam o GDPR; e (c) quaisquer outras leis ou regulamentos aplicáveis relacionados ao processamento e proteção de Dados Pessoais para os fins deste Contrato.
- "Violação de Proteção de Dados" significa uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos Dados Pessoais Processados do Cliente para os propósitos deste DPA.
- “Dados Pessoais” designa qualquer informação relativa a uma pessoa física identificada ou identificável (“Titular dos dados”); uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, em

particular por referência a um número de identificação ou a um ou mais fatores específicos de sua identidade física, fisiológica, mental, econômica, cultural ou social.

- “Processamento” ou “Processos” significa qualquer operação ou conjunto de operações que são realizadas nos Dados Pessoais, seja ou não por meios automáticos, como coleta, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição.
- "Processador" significa a pessoa ou entidade que Processa os Dados Pessoais em nome do Cliente, conforme contemplado pelo Contrato e este DPA
- “Controlador” significa a pessoa jurídica ou entidade que, isoladamente ou em conjunto com outros, determina as finalidades e meios do Processamento de Dados Pessoais. No contexto dos Serviços em Nuvem da Unify sob este DPA, concorda-se, conforme descrito acima, que as Partes compartilham as funções e responsabilidades de um Controlador da seguinte maneira:
  - O Cliente (i) é responsável por definir os objetivos do Processamento de Dados Pessoais, (ii) é responsável pela exatidão dos Dados Pessoais, (iii) é responsável por informar os titulares dos dados sobre o processamento de Dados Pessoais e as modalidades para o exercício de seus direitos, e (iv) é responsável por elaborar notificações (incluindo notificações de violação de proteção de dados) às autoridades de proteção de dados, se necessário.
  - A Unify (i) define os meios do Processamento e (ii) é responsável pela implementação das medidas de segurança.

2 Categorias de dados pessoais sob este DPA:

As seguintes categorias de Dados Pessoais são geralmente coletadas e processadas pela Unify para executar os Serviços sob o TOSP:

- Dados do perfil: Os Dados Pessoais dos Usuários dos Serviços em Nuvem da Unify (Usuários) criam, em particular, seu nome de usuário, senha, endereço de e-mail, direitos de acesso;
- Dados da atividade: Dados pessoais derivados do uso dos Serviços em Nuvem da Unify pelos usuários, em especial os dados do diário de chamadas, exclusão ou alteração de conteúdo ou dados relacionados ao uso do serviço (por exemplo, endpoints usados) por um usuário, na medida em que tais dados não foram anonimizados para gerar Dados de Uso agregados;
- Dados transitórios e de sessão: Dados pessoais que não são armazenados nos Serviços em Nuvem da Unify (como informações de presença ou localização) ou que estão vinculados a uma sessão de logon nos Serviços em Nuvem da Unify (por exemplo, endereços de IP).

Excluídos deste DPA estão as seguintes categorias de dados pessoais:

- Dados pessoais de terceiros que os Usuários dos Serviços em Nuvem da Unify podem inserir nos Serviços em Nuvem da Unify por meio de publicações de texto, upload de documentos ou gravações de voz. Esses dados não podem ser reconhecidos pelos Serviços em Nuvem da Unify como Dados Pessoais.
- Dados pessoais de terceiros que os Usuários dos Serviços em Nuvem da Unify podem inserir em seus dispositivos telefônicos, como em catálogos de endereços privados. Esses dados não são armazenados ou processados pelos Serviços em Nuvem da Unify, mas estão presentes apenas no telefone dos Usuários, fora dos Serviços em Nuvem da Unify.
- O Cliente é aconselhado a controlar o uso com relação a tais Dados Pessoais dos Serviços em Nuvem da Unify através de políticas apropriadas de proteção de dados.

3 Categorias de Titulares dos Dados sob este DPA:

As seguintes categorias de Titulares dos Dados são afetadas pelo processamento de seus Dados Pessoais dentro da estrutura deste DPA:

- Usuários da Conta de Subscrição de Serviços em Nuvem da Unify, contratados pelo Cliente;

- Usuários Cruzados com acesso à Conta de Subscrição dos Serviços em Nuvem da Unify, contratados pelo Cliente (somente Dados da atividade mantidos na Conta de Subscrição dos Serviços em Nuvem da Unify, contratados pelo Cliente);
- Usuários Convidados da Sessão com acesso à Sessão de Serviços em Nuvem da Unify, contratados pelo Cliente.

4 Funções e Responsabilidades do Cliente e da Unify

4.1 Função e Responsabilidades do Cliente:

4.1.1 **Finalidade e Legalidade do Processamento:** O Cliente será responsável por definir a finalidade do Processamento de Dados Pessoais, para a legalidade da transferência de Dados Pessoais para a Unify e para legalidade do Processamento de Dados. O Cliente deverá cumprir, e fará com que suas Afiliadas e contratadas cumpram, com todas as suas obrigações sob as Leis de Proteção de Dados ao processar Dados Pessoais em conexão com os Serviços em Nuvem. A este respeito, o Cliente deverá assegurar, particularmente, a obtenção e manutenção de todos os registros ou autorizações necessárias junto às autoridades competentes em matéria de proteção de dados e dos fundamentos legais válidos para o processamento de Dados Pessoais.

4.1.2 **Direitos de exercício dos Titulares dos Dados:** O Cliente será o contato principal para os Titulares dos Dados exercerem seus direitos conforme a Legislação de Proteção de Dados aplicável. Consulte o artigo 4.2.9 sobre as responsabilidades da Unify neste contexto.

4.1.3 **Precisão, Qualidade, Legalidade, Confiabilidade dos Dados Pessoais:** O Cliente terá a responsabilidade exclusiva pela precisão, qualidade, legalidade e confiabilidade dos Dados Pessoais e dos meios pelos quais ele adquire os Dados Pessoais para o processamento pelos Serviços em Nuvem da Unify.

4.1.4 **Gerenciamento de Riscos**: O Cliente será responsável pela avaliação dos riscos resultantes do Processamento de Dados Pessoais.

4.1.5 **Registros do Processamento:** na medida exigida pela lei aplicável, o Cliente será responsável por conservar e manter os Registros de Processamento para os Controladores com respeito a todas as obrigações do Controlador atribuídas ao Cliente por este DPA. Consulte também o artigo 4.2.1, 4.2.3, e 4.2.14 sobre as responsabilidades da Unify neste contexto, bem como o artigo 4.1.12.

4.1.6 **Informações dos Titulares dos Dados:** O Cliente será responsável por fornecer as informações aos Titulares dos Dados sobre o processamento dos Dados Pessoais, conforme exigido pela Legislação de Proteção de Dados aplicável. Consulte também o artigo 4.2.1 e 4.2.3 sobre as responsabilidades da Unify neste contexto, bem como o artigo 4.1.12.

4.1.7 **Informações sobre a Divisão de Responsabilidades do Controlador/Co-Controlador para os Titulares dos Dados:** O Cliente é responsável por informar ao Titular dos Dados sobre a divisão de responsabilidade entre o Controlador e o Co-Controlador, de acordo com este DPA. Consulte o artigo 4.2.4 sobre a responsabilidade da Unify neste contexto.

4.1.8 **Notificação de Violação de Proteção de Dados:** O Cliente deverá cumprir todas as obrigações de notificação de violação de Proteção de Dados resultantes dos requisitos de Proteção de Dados aplicáveis. Quando imposta pela Lei de Proteção de Dados aplicável, o Cliente é responsável pela notificação da Violação da Proteção de Dados aos Titulares dos Dados e às Autoridades de Proteção de Dados. Consulte também 4.2.5 sobre as responsabilidades da Unify neste contexto.

4.1.9 **Mudanças na Legislação Aplicável:** O Cliente deve notificar a Unify em tempo hábil sobre as mudanças nos regulamentos legais que possam afetar os deveres contratuais da Unify sob este DPA e que podem exigir a alteração deste DPA e a remuneração acordada. A Unify também pode enviar propostas ao Cliente se ela considerar que determinada alteração é necessária para permanecer em conformidade com a Lei Aplicável.

4.1.10 **Irregularidades ou Erros no Processamento de Dados Pessoais:** O Cliente informará à Unify, imediata e detalhadamente, sobre quaisquer erros ou irregularidades relacionadas às Leis de Proteção de Dados no Processamento de Dados Pessoais de que tenha conhecimento.

4.1.11 **Notificação sobre retificação, exclusão, dados pessoais ou restrição de processamento aos destinatários de dados pessoais:** A Unify não divulga os Dados Pessoais para qualquer outra finalidade que não seja para o Processamento necessário para o fornecimento dos Serviços em Nuvem da Unify (consulte a seção 8). Na medida em que o Cliente divulga os Dados Pessoais a um destinatário, por exemplo, integrando os Serviços em Nuvem da Unify com outros serviços em nuvem, transmitindo Dados Pessoais através de interfaces do Circuit fora do Circuit, o Cliente é obrigado a notificar tais destinatários sobre solicitações de retificação ou exclusão de Dados Pessoais divulgados ou uma restrição de Processamento dos Titulares dos Dados.

4.1.12 **Divulgação de dados pessoais:** A Unify divulga os Dados Pessoais somente para os destinatários aos quais é necessário divulgar os Dados Pessoais para fins de processamento. Consulte "Informações sobre Processamento" em https://unify.com/br/informacoes-legais/dps-para-circuit para detalhes. Certos recursos dos Serviços em Nuvem da Unify permitem que clientes e usuários divulguem Dados Pessoais para terceiros. Na medida em que o Cliente ou os usuários do Cliente aproveitam esses recursos, o Cliente é responsável por informar os Titulares dos Dados (artigo 4.1.6) e por incluir tal uso nos Registros de Processamento (artigo 4.1.5).

4.2 Função e Responsabilidades da Unify

4.2.1 **Meios de Processamento:** A Unify será responsável pela definição dos meios de Processamento e, em referência aos artigos 4.1.5 e 4.1.6, fornecer informações sobre esses meios ao Cliente, especificamente para permitir que o Cliente conclua os Registros de Processamento e para informar os Titulares dos Dados conforme exigido pela Legislação de Proteção de Dados aplicável. Esta "Informação sobre Processamento" é apresentada em https://unify.com/br/informacoes-legais/dps-para-circuit.

4.2.2 **Escopo do processamento pela Unify:** A Unify pode coletar e processar os Dados Pessoais somente dentro da estrutura deste DPA e dos TOSP aplicáveis aos Serviços em Nuvem da Unify fornecidos ao Cliente, e para melhorar e atualizar esses serviços. Alterações materiais no escopo do Processamento de Dados devem ser acordadas em conjunto e devem ser documentadas. Através do presente DPA, a Unify reconhece expressamente que deve processar os Dados Pessoais somente para o fornecimento dos Serviços em Nuvem da Unify, bem como para a melhoria e atualização de tais Serviços.

4.2.3 **Implementação de medidas de segurança**: A Unify será responsável pela implementação de medidas de segurança para o Processamento de Dados Pessoais no âmbito dos Serviços em Nuvem da Unify. A Unify tomará as Medidas Técnicas e Organizacionais (TOMs) apropriadas, conforme estabelecido no Apêndice 1 deste DPA, destinadas a proteger os Dados Pessoais do Cliente contra uso indevido e perda, ou contra qualquer outra violação de proteção de dados, de acordo com as Leis de Proteção de Dados aplicáveis. O cliente entende que os TOMs estão sujeitos a um progresso técnico e desenvolvimento adicional. A este respeito, a Unify poderá usar medidas alternativas adequadas, e informando os clientes, disponibilizando uma descrição dessas medidas mediante solicitação. Em referência aos artigos 4.1.5 e 4.1.6, fornecer informações sobre esses TOMs ao Cliente, especificamente para permitir que o Cliente preencha registros de processamento e para informar os Titulares dos Dados, conforme exigido pela Lei de Proteção de Dados Aplicável.

4.2.4 **Informações sobre a Divisão de Responsabilidades das Partes aos Titulares dos Dados:** A Unify é responsável por tornar o DPA acessível a todos os usuários dos Serviços em Nuvem da Unify. A Unify não terá a responsabilidade de comunicar eventuais alterações no DPA aos Titulares dos Dados.

4.2.5 **Notificação de Violação de Proteção de Dados:** No contexto do artigo 4.1.8, no caso de uma Violação de Proteção de Dados, a Unify deverá auxiliar o Cliente e fornecer todas as informações necessárias a que tenha acesso, a fim de permitir que o Cliente cumpra suas obrigações. A Unify notificará o Cliente, sem demora indevida, sobre qualquer violação dos Dados Pessoais do Cliente descoberta pela Unify.

4.2.6 **Retenção de Dados Pessoais / Limitação para exclusão:** Os Dados Pessoais processados pelos Serviços em Nuvem da Unify são geralmente retidos até que a) sejam excluídos pelo Cliente ou pelos Usuários dos Serviços em Nuvem da Unify, ou b) um período de retenção tenha expirado, ou c) o contrato de serviços em nuvem do Cliente para os Serviços em Nuvem da Unify seja encerrado (consulte o artigo 4.2.7 sobre encerramento). O Cliente não pode exigir a exclusão de Dados Pessoais, uma vez que uma Lei ou regras aplicáveis exija que a Unify mantenha materiais que contenham esses Dados Pessoais. Quando a Unify precisar reter Dados Pessoais por tais razões, seu processamento será restrito pela Unify, ou terceiros por ela contratados, até que o período de retenção

aplicável tenha expirado. Além disso, o processamento dos Dados Pessoais será restrito em vez de excluir os Dados Pessoais, na extensão legalmente permitida pela Lei de Proteção de Dados Aplicáveis, em particular, se a exclusão não for razoavelmente viável ou se for somente possível com um custo desproporcional devido ao tipo específico de armazenamento. O Cliente reconhece e aceita que algumas solicitações podem resultar em reivindicações de remuneração adicionais para a Unify. A Unify informará o Cliente antes de executar a solicitação.

4.2.7 **Exclusão e Exportação de Dados Pessoais após a Rescisão do Contrato de Serviços em Nuvem:** A Unify será responsável por excluir todos os dados inseridos pelo Cliente e pelos Usuários dos Serviços em Nuvem da Unify nos aplicativos do Software fornecidos pelos Serviços em Nuvem da Unify ("Dados da Conta de Subscrição"), incluindo os Dados Pessoais ao final do mês civil após a expiração ou término do uso do Cliente dos Serviços em Nuvem da Unify, ou a qualquer momento, mediante solicitação do Cliente. Mediante solicitação do Cliente, a Unify fornecerá uma exportação de Dados de Arrendamento em um formato de dados que pode ser processado pelo Cliente para portabilidade para outros serviços da Nuvem. Para exceções e limitações: consulte o artigo 4.2.6.

4.2.8 **Solicitações de Clientes sobre Dados Pessoais:** A Unify será responsável por atender às solicitações do Cliente para correção, exclusão, restrição e disponibilização de Dados Pessoais durante a vigência e no término do Contrato. Para exceções e limitações, consulte o artigo 4.2.6

4.2.9 **Direitos de exercício dos Titulares dos Dados:** Caso a Unify receba uma solicitação para o exercício de direitos de um Titular de Dados conforme a Lei de Proteção de Dados Aplicável, a Unify encaminhará essa solicitação ao Cliente, que instruirá a Unify sem atrasos indevidos sobre como proceder. O Cliente reconhece que, em caso de conflito entre o Titular de Dados e o Cliente, a legislação aplicável pode forçar a Unify a atender à solicitação do Titular dos Dados com relação à objeção do Cliente. A Unify, entretanto, não tomaria essa medida sem a devida consideração da situação legal juntamente com o Cliente.

4.2.10 **Efeitos da Exclusão dos Dados Pessoais:** O Cliente por meio deste material confirma e reconhece que, caso o Cliente solicite à Unify a exclusão dos Dados Pessoais ou a restrição de seu Processamento, isto pode tornar impossível o fornecimento dos produtos ou dos serviços fornecidos ou contratados. A Unify notificará o Cliente sobre tal consequência antes da execução de tal solicitação.

4.2.11 **Cópias de backup de Dados Pessoais:** A Unify fará cópias de segurança dos Dados Pessoais na medida em que eles sejam necessários para garantir o processamento correto dos Dados Pessoais, e poderá copiar e manter os Dados Pessoais necessários para a conformidade com as obrigações estatutárias de retenção de documentos do Cliente ou da Unify.

4.2.12 **Manuseio de mídia e material de teste:** A Unify armazenará e controlará a mídia fornecida à Unify e todas as cópias ou reproduções da mesma, com cuidado, para que não sejam acessadas por terceiros. A Unify será obrigada a providenciar a destruição de material de teste e outros materiais que contenham Dados Pessoais que devam ser descartados de uma maneira compatível com a lei somente com base em uma solicitação individual do Cliente e às custas deste.

4.2.13 **Especialista de Proteção de Dados (Data Protection Officer):** A Unify fornecerá os detalhes de contato do Data Protection Officer na Internet. A partir da Data de Vigência deste DPA, os detalhes de contato atuais do DPO estão em dp.it-solutions@atos.net.

4.2.14 **Registros do Processamento:** A Unify será responsável por conservar e manter os Registros de Processamento para os Processadores para toda as responsabilidades dos Controladores e atribuídas à Unify, através deste DPA. Consulte o artigo 4.1.5 sobre as responsabilidades do Cliente neste contexto. A Unify disponibilizará as respectivas informações em "Informações sobre Processamento: https://unify.com/br/informacoes-legais/dps-para-circuit

5 Acordos e Responsabilidades Mútuas

5.1 As Partes concordam que quaisquer solicitações referentes a Dados Pessoais emitidos pelo Cliente deverão ser elaboradas de forma escrita e explícita. Caso tais solicitações exijam uma alteração nos serviços, tais alterações serão renegociadas de boa-fé por ambas as Partes, bem como o preço relacionado.

5.2 Cada uma das Partes deve assegurar que a respectiva equipe esteja vinculada por uma obrigação legal de cumprimento das obrigações em matéria de Proteção de Dados e de confidencialidade dos dados e que seja informada

sobre outras disposições aplicáveis em matéria de proteção de Dados Pessoais, em especial o sigilo das telecomunicações. A obrigação de manter o sigilo dos dados continua a ser aplicada após o término do contrato de trabalho ou de vínculo empregatício.

5.3 Se houver indício que as solicitações do Cliente possam resultar em uma violação das Leis de Proteção de Dados aplicáveis, a Unify deve notificar imediatamente o Cliente a respeito de tal violação. A Unify terá o direito de suspender a implementação da solicitação relevante até que ela seja alterada pelo Cliente.

5.4 Ambas as Partes reconhecem que as medidas de segurança detalhadas no Apêndice 1 (Medidas Técnicas e Organizacionais) fornecem garantias suficientes para os Dados Pessoais Processados. O cliente entende que as medidas técnicas e organizacionais estão sujeitas a progresso técnico e desenvolvimento adicional. A este respeito, a Unify poderá usar medidas alternativas e adequadas.

5.5 Caso os Dados Pessoais do Cliente fiquem sujeitos a busca e apreensão, ordem de penhora, confisco durante falência ou processo de insolvência, eventos ou medidas semelhantes de terceiros, a Unify informará o Cliente sem demora, se permitido por lei. A Unify deve, imediatamente, notificar todas as partes pertinentes em tal ação que os Dados Pessoais afetados por suas medidas são de propriedade exclusiva do Cliente e sob disposição única do Cliente, e que o Cliente é o exclusivo responsável, nos temos da Lei de Proteção de Dados Aplicável.

6 Pedidos das Autoridades Regulatórias

6.1 Quando exigido por lei, ambas as Partes devem manter os registros dos Dados Pessoais processados para os propósitos deste DPA, cooperar e fornecer todas as informações necessárias para o cumprimento das obrigações acima e o dever de notificação sob a Lei de Proteção de Dados Aplicáveis.

6.2 Se a Unify tiver que ajudar o Cliente a cumprir as obrigações legais do Cliente, conforme estabelecido na seção 6, o Cliente deverá reembolsar a Unify com respeito a quaisquer custos adicionais razoáveis associados à prestação de tal assistência.

7 Direito à Auditoria

7.1 Não mais de uma vez por ano e com 60 (sessenta) dias de antecedência, cada Parte terá o direito de realizar uma auditoria sobre o cumprimento da outra Parte com esse DPA, revendo as medidas técnicas e organizacionais implementadas pela parte auditada. A evidência para a implementação de tais medidas que não se relacionam exclusivamente com este DPA específico ou o Contrato também pode ser fornecida através da apresentação de um certificado atual, relatórios ou trechos de relatórios de terceiros independentes, por ex. por contadores públicos, auditores de conta, encarregados de proteção de dados internos e/ou externos da parte auditada, departamento de segurança de TI, auditores internos e externos de proteção de dados, auditores de qualidade ou por um certificado apropriado emitido após a segurança de TI da Parte auditada ou a proteção de dados ter sido auditada por terceiros.

7.2 Cada Parte reserva-se o direito de recusar-se a fornecer à outra Parte os segredos comerciais e de negócios, know-how operacional e qualquer informação cuja auditoria represente um risco de segurança para a Parte auditada ou seus clientes, ou que a Parte auditada esteja proibida de fornecer ou divulgar tais como dados protegidos por lei ou os dados de outros clientes.

8 Sub-processadores

8.1 O Cliente reconhece e aceita que a Unify pode subcontratar, no todo ou em parte, a execução dos Serviços em Nuvem da Unify. Tais subcontratantes podem ser entidades do Grupo Atos (“Subcontratantes internos”) ou terceiros subcontratados (“Subcontratantes Externos”). Uma lista completa de subcontratantes aprovados a partir da Data de Vigência deste DPA é fornecida em https://unify.com/br/informacoes-legais/dps-para-circuit incluindo as salvaguardas aplicáveis para a proteção adequada dos Dados Pessoais.

8.2 Caso a Unify pretenda contratar um novo subcontratado externo que não esteja identificado na lista de subcontratados aprovados na Data de Vigência deste DPA, os artigos 9.2 e 9.3 devem ser aplicados. Para evitar dúvidas, é expressamente acordado que os Subcontratantes Internos não serão regidos por esta disposição e o Cliente não

deve se opor ao uso de Subcontratados Internos.

8.3 Transferências de dados pessoais para países terceiros:

8.3.1 O Cliente reconhece e aceita expressamente que os Dados Pessoais podem ser transferidos e/ou processados por Subcontratados Externos, conforme previsto no artigo 8.1 acima, inclusive quando esses Subcontratados Externos estiverem localizados fora da Área Econômica Europeia (EEA).

8.3.2 Os Subcontratantes Internos fazem parte do Grupo Atos e, portanto, estão vinculados às Regras Corporativas Vinculantes, conforme aprovadas pelas autoridades europeias de proteção de dados e que estão disponíveis em https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf (a "BCR"). O Cliente reconhece que, caso a Unify transfira os Dados Pessoais para qualquer entidade do grupo Atos localizado fora da EEA, a BCR constituirá uma salvaguarda suficiente para estabelecer que tais entidades fornecem uma proteção adequada aos Dados Pessoais, conforme exigido pela Lei de Proteção de Dados Aplicáveis. Consequentemente, o Cliente consente expressamente que os Dados Pessoais possam ser transferidos para qualquer uma das entidades do Grupo Atos vinculadas aos termos da BCR, conforme listado no Anexo 2 da BCR. A Unify disponibilizará por qualquer meio apropriado ao Cliente qualquer atualização ao Apêndice 2 da BCR. O Cliente se compromete a fornecer informações adequadas aos Titulares dos Dados sobre a BCR.

8.3.3 Se a Unify transferir os Dados Pessoais para um Subcontratado externo localizado fora da EEA que não se enquadra no escopo da BCR, o Cliente, por meio do presente, concede expressamente à Unify uma autorização para celebrar quaisquer acordos relevantes para assegurar que a entidade destinatária implemente um nível adequado de proteção para Dados Pessoais reconhecidos como apropriados pelas autoridades competentes europeias ou locais.

9 Alterações a este DPA

9.1 O Cliente reconhece que os termos neste DPA e no Apêndice 1 estão sujeitos a alterações pela Unify. Uma alteração requer o consentimento do Cliente se a) isso afetar a divisão de responsabilidade entre o Controlador e o Co-Controlador, conforme a seção 4, ou b) isso limitar os direitos do Cliente ou c) isso exigir um consentimento conforme a Lei de Proteção de Dados Aplicável. Em outros casos, uma alteração requer apenas informações para o Cliente.

9.2 No caso de uma alteração que exija o consentimento do Cliente, a Unify notificará o Cliente sobre a alteração via e-mail ao administrador do arrendatário sob o qual o Arrendamento do Serviço em Nuvem do Cliente está registrado na Unify ou por meio do parceiro de vendas credenciado da Unify com quem o Cliente detém o contrato de Serviços em Nuvem para um Serviço em Nuvem da Unify, e disponibilizará as informações relevantes ao Cliente para análise pelo menos trinta (30) dias antes da alteração entrar em vigor. A Unify dará ao Cliente a oportunidade de dar o seu consentimento ou de se opor. Se nenhuma objeção do Cliente for recebida pela Unify após um período de resposta indicado na notificação de alteração, que será de no mínimo 10 (dez) dias corridos após a data da notificação, o consentimento do Cliente será considerado como dado. Em situações de emergência, os períodos de notificação e resposta podem ser mais curtos.

9.3 O Cliente não se oporá a uma alteração sem fornecer à Unify uma explicação detalhada por escrito dos motivos para tal objeção. A Unify empreenderá esforços comercialmente razoáveis para tratar as preocupações do Cliente. Ambas as Partes cooperarão de boa-fé para chegar a um acordo. Se nenhum acordo puder ser obtido, os Serviços em Nuvem da Unify contratados pelo Cliente serão encerrados.

10 Responsabilidade

10.1 A Unify e o Cliente deverão cumprir suas respectivas obrigações, conforme estabelecido neste DPA e na Lei de Proteção de Dados Aplicáveis.

10.2 O Cliente terá total responsabilidade por qualquer violação de suas obrigações na seção 4.1 acima, bem como por suas obrigações, conforme estabelecido na seção 5 acima.

10.3 A Unify terá total responsabilidade por qualquer violação de suas obrigações segundo a seção 4.2 acima, bem como por suas obrigações, conforme estabelecido na seção 5 acima, sujeita a qualquer sujeição do Cliente.

10.4 Quando estiver atuando como o Processador, a Unify será responsável pelos danos causados pelo processamento somente quando não cumprir com as obrigações da Lei de Proteção de Dados Aplicáveis dirigida aos processadores ou se ela tiver agido fora ou contrária às instruções legais do Cliente.

10.5 A Parte infratora estará isenta de responsabilidade se provar que não é de forma alguma responsável pelo evento que deu origem ao dano.

10.6 Quando o Cliente e a Unify forem responsáveis por qualquer dano causado em violação de uma obrigação neste DPA, cada Parte será responsabilizada por todo o dano, a fim de garantir uma compensação efetiva do Titular dos Dados. A Parte que pagou a indenização integral pelos danos sofridos terá direito a restituir da outra parte, a parte da indenização correspondente à sua parte de responsabilidade pelos danos (direito de regresso).

11 Disposições Diversas

11.1 Se qualquer disposição individual do DPA for ilegal, inválida, nula, anulável ou inexequível, o restante do DPA continuará em pleno vigor e efeito. As Partes acordarão uma disposição eficaz que, na medida legalmente possível, reflita rigorosamente a intenção das Partes.

Apêndice 1

Medidas Técnicas e Organizacionais Gerais da Unify

Na Unify, as medidas técnicas e organizacionais exigidas por lei são implementadas com base na Estrutura de Privacidade de Dados e Segurança da Informação da Unify (a “Estrutura DIS”), que define padrões de política (nível 2) e procedimentos operacionais (nível 3) de acordo com a norma internacional ISO27001 com base na política corporativa da Unify “Política de Privacidade de Dados e de Segurança da Informação". Os documentos estão disponíveis para o Cliente mediante solicitação.

A seguinte descrição do status quo das medidas elementares relativas à proteção de dados não pode abranger todas e quaisquer medidas de segurança em vigor na Unify. Em particular, no contexto da proteção de dados e da segurança dos dados, também não é viável fornecer descrições detalhadas de medidas confidenciais, uma vez que a proteção das medidas de segurança contra a divulgação não autorizada é tão importante quanto a própria medida de segurança.

O Cliente é incentivado a discutir quaisquer questões individuais relacionadas às medidas técnicas e organizacionais com o gerente de contas do Cliente na Unify, no DPO da Unify e, quando relevante, com o Chief Information Officer (Diretor de Informações) (CISO) da Unify.

1. Controle de Entrada

Medidas técnicas ou organizacionais relativas ao controle de acesso, especialmente em relação à legitimação de pessoas autorizadas:

O objetivo do controle de entrada é impedir que pessoas não autorizadas acessem fisicamente esse equipamento de processamento de dados que processa ou usa Dados Pessoais.

Devido a seus respectivos requisitos de segurança, as unidades e instalações comerciais são subdivididas em diferentes zonas de segurança com diferentes autorizações de acesso. Elas são monitoradas pelo pessoal de segurança. O acesso para funcionários somente é possível com um ID codificado com uma foto nele. Todas as outras pessoas têm acesso somente após terem se registrado antes (por exemplo, na entrada principal).

O acesso a áreas especiais de segurança, como o centro de serviços para manutenção remota, é protegido adicionalmente por uma área de acesso separada. Os padrões de segurança construtivos e substantivos atendem aos requisitos de segurança para centros de dados

2. Controle de acesso ao sistema

Medidas técnicas (proteção por senha) e organizacionais (dados mestres do usuário) com relação ao ID do usuário e a autenticação:

O objetivo do controle de acesso do sistema é evitar o uso não autorizado de sistemas de processamento de dados que são usados para o processamento e o uso de Dados Pessoais.

Os dados mestres do usuário e o código de identificação individual de cada funcionário são registrados no diretório global de contatos. A admissão aos sistemas de processamento de dados é possível somente após a identificação e autenticação, utilizando o código de identificação e a senha para o sistema em particular.

Proteções técnicas adicionais estão em vigor usando firewalls e servidores proxy.

Para garantir o controle de admissão, tecnologias de criptografia são usadas (por exemplo, acesso remoto à rede da empresa via túnel VPN). A adequação de uma tecnologia de criptografia é medida com relação ao propósito de proteção.

3. Controle de Acesso aos Dados

Estrutura sob demanda do conceito de autorização e dos direitos de acesso aos dados, bem como seu monitoramento e registro:

As medidas relativas ao controle de acesso a dados devem ser levar em conta que apenas esses dados podem ser

acessados, para os quais existe uma autorização de acesso, e que os Dados Pessoais não podem ser lidos, copiados, alterados ou excluídos de forma não autorizada durante o processamento, uso e após o salvar tais dados.

O acesso aos dados necessários para o desempenho da tarefa específica é assegurado dentro dos sistemas e aplicativos por meio de uma função e conceito de autorização correspondentes. De acordo com o princípio da "necessidade de saber", cada função tem apenas os direitos necessários para o cumprimento da tarefa a ser desempenhada pelo indivíduo.

Para garantir o controle de acesso aos dados, é utilizada uma tecnologia de criptografia (por exemplo, acesso remoto à rede da empresa via túnel VPN). A adequação de uma tecnologia de criptografia é medida com relação ao propósito de proteção.

4. Controle de Transmissão

Medidas relativas ao transporte, transferência, transmissão ou armazenamento de Dados Pessoais em mídias de dados (manual ou eletronicamente), bem como em relação à revisão subsequente:

O objetivo do controle de transmissão é garantir que os Dados Pessoais não possam ser lidos, copiados, alterados ou excluídos sem autorização durante sua transferência ou enquanto armazenados em mídia de dados, e que possam ser monitorados e determinados para quais destinatários uma transferência de Dados Pessoais destina-se.

As medidas necessárias para garantir a segurança dos dados durante o transporte, a transferência e a transmissão dos Dados Pessoais, bem como quaisquer outros dados da empresa ou do cliente, estão detalhadas na política de proteção de informações comerciais confidenciais. Nesta política, há uma descrição detalhada de todo o processamento de dados, desde a criação de tais dados até a sua exclusão, incluindo o tratamento de tais dados de acordo com sua classificação.

Para garantir o controle de transferência, é utilizada uma tecnologia de criptografia (por exemplo, acesso remoto à rede da empresa via túnel VPN). A adequação de uma tecnologia de criptografia é medida com relação ao propósito de proteção.

A transferência de Dados Pessoais para terceiros (por exemplo, clientes, subcontratados, prestador de serviços) somente é feita se existir um contrato correspondente e apenas para uma finalidade específica. Se os Dados Pessoais forem transferidos para empresas com sede fora da UE/EEE, a Unify deve estabelecer que exista um nível adequado de proteção de dados no local ou organização de destino, de acordo com os requisitos de proteção de dados da União Europeia, por ex. através da contratação de contratos baseados nas cláusulas contratuais modelo da UE.

5. Controle de Entrada de Dados

Medidas relativas à revisão subsequente, se e por quem os dados foram inseridos, alterados ou excluídos:

O objetivo do controle de entrada de dados é garantir, com a ajuda de medidas apropriadas, que as circunstâncias da entrada de dados possam ser revisadas e monitoradas retroativamente.

As entradas do sistema são registradas na forma de arquivos de registros. Ao fazer isso, é possível em um estágio posterior revisar se e por quem os Dados Pessoais foram inseridos, alterados ou excluídos.

6. Controle de Processamento dos Dados

O objetivo do controle de processamento de dados é garantir que a Unify processe os Dados Pessoais somente de acordo com os Termos de Produção de Serviço (ToSP) emitidos pela Unify para o serviço em nuvem contratado e com as disposições estabelecidas no Contrato de Processamento de Dados (DPA) para os Serviços em Nuvem da Unify.

Dados pessoais processados nos Serviços em Nuvem da Unify acessíveis apenas ao suporte técnico e à organização da operação. A Unify possui políticas em vigor para impedir que esta organização use Dados Pessoais para qualquer outra finalidade ou para divulgar Informações Pessoais a qualquer outra organização ou terceiros, exceto mediante instruções do Cliente.

Uma transferência de Dados Pessoais para um terceiro, como um subcontratado, é feita apenas sob consideração das disposições contratuais e da Lei de Proteção de Dados Aplicável.

7. Controle de disponibilidade

Medidas relativas ao backup de dados (físico/lógico):

O objetivo do controle de disponibilidade é garantir que os Dados Pessoais sejam protegidos contra destruição e perda acidentais.

Se os Dados Pessoais não forem mais necessários para os propósitos para os quais foram processados, serão excluídos imediatamente. Deve-se observar que, a cada exclusão, os Dados Pessoais são bloqueados apenas na primeira instância e, em seguida, são excluídos definitivamente com um certo atraso. Isso é feito para evitar exclusões acidentais ou possíveis danos intencionais.

Devido a razões técnicas, as cópias dos Dados Pessoais podem estar presentes em arquivos de backup e podem ser feitas pelo espelhamento de serviços. Sujeitas à obrigação legal de retenção de dados da Unify (consulte Contrato de processamento), tais cópias também são excluídas - se necessário, com um atraso tecnicamente causado. A disponibilidade dos próprios sistemas é assegurada de acordo com o nível de segurança necessário por medidas de segurança correspondentes (por exemplo, espelhamento de discos rígidos, sistemas RAID, USV).

8. Controle de Separação

Medidas relativas ao processamento separado (salvar, alterar, excluir e transferir) de dados com finalidades diferentes:

O objetivo do controle de separação é garantir que os dados coletados para diferentes finalidades possam ser processados separadamente.

Os dados pessoais são usados apenas para fins internos (por exemplo, como parte do respectivo relacionamento com o cliente). Uma transferência para um terceiro, como um subcontratado, é feita exclusivamente sob consideração de disposições contratuais e regulamentos de proteção de dados.

Os funcionários são instruídos a coletar, processar e usar os Dados Pessoais somente dentro da estrutura e para os objetivos de suas funções (por exemplo, prestação de serviços). Em um nível técnico, a capacidade de vários clientes, a separação de funções, bem como a separação de sistemas de teste e produção, são usadas para essa finalidade.

8.1. Procedimentos adicionais para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento (Art. 32 Seção 1 lit. d GDPR; Art. 25 Seção 2 GDPR)

8.2. Gerenciamento da Proteção de Dados

A proteção de dados na Atos é organizada em uma empresa global com funcionários de proteção de dados e especialistas jurídicos para as Unidades de Negócios Globais (GBUs) e países.

A GBU Alemanha possui um escritório de proteção de dados com três Oficiais de Proteção de Dados e pelo menos um especialista legal. O Escritório de Proteção de Dados faz parte da organização de proteção de dados e segurança da informação, que regularmente troca seus tópicos.

A Política de Proteção de Dados do Grupo é a base para a proteção de dados na Atos, que descreve os princípios de proteção de dados, bem como os processos relativos aos direitos das pessoas envolvidas, auditorias, treinamento e conscientização e se refere à política global de segurança da informação com seus regulamentos adicionais.

O Escritório de Proteção de Dados fornece documentos predefinidos no Sistema Integrado de Gerenciamento da Atos (AIMS), como formulários, listas de verificação, manuais e instruções de trabalho usados em processos de negócios e RH. Todos os funcionários estão comprometidos com o sigilo de dados e com a observância dos segredos comerciais e da empresa e dependentes do GDPR, Artigos 29 e 32 (4) para processar dados pessoais somente seguindo as instruções do controlador de dados. Além disso, eles foram obrigados a cumprir a Lei das Telecomunicações (Seção 88) e, se apropriado, a salvaguardar o sigilo social e/ou o sigilo bancário.

Em sessões de treinamento anuais obrigatórias, os funcionários da Atos devem atualizar sua conscientização sobre a privacidade.

As medidas técnicas e organizacionais de proteção de dados em conformidade com o GDPR, Artigo 32, são revisadas regularmente dentro do escopo da certificação ISO e das auditorias ISAE3402. Além disso, as auditorias internas de processo também levam em consideração questões relevantes à proteção de dados.

8.3. Gerenciamento de riscos e segurança

A Atos conduz seus serviços com base em um sistema de gerenciamento de segurança. Isso inclui, entre outras coisas, diretrizes e instruções documentadas para a operação de TI/Centro de Dados. Eles se baseiam em regulamentações estatutárias e internas. Os processos de segurança utilizados são verificados regularmente. As diretrizes também são vinculativas para os subcontratantes. Os funcionários da Atos são treinados anualmente em sessões de treinamento obrigatórias sobre a conscientização de segurança.

A Atos implementou um processo de gerenciamento de riscos em todos os níveis da empresa e nomeou gerentes de risco dedicados em vários níveis da organização para garantir a implementação do gerenciamento de riscos.

Os processos de gerenciamento de riscos são divididos em gerenciamento de risco operacional, que é relevante para propostas, contratos (desde a transferência do serviço para a Atos, o início do projeto até a conclusão do projeto ou o término do serviço) e a área operacional, ou seja, os locais, serviços e processos relevantes.

Os riscos, a sua avaliação e o acompanhamento das medidas definidas são documentados em registros de risco e revistas e atualizadas regularmente pelos responsáveis, com o envolvimento do gestor de riscos responsável e dos especialistas relevantes. Os controles são definidos e documentados com respeito a todos os riscos inerentes ao negócio. Para cada um desses controles existem responsáveis para monitorar regularmente a eficácia.

8.4. Certificação

As empresas alemãs Atos são certificadas de acordo com

- DIN EN ISO 9001: 2015 (Gestão da Qualidade)

- ISO / IEC 27001: 2013 (Gestão de Segurança da Informação)

- ISO / IEC 20000-1: 2011 (Gestão de Serviços de TI)

por Ernst & Young CertifyPoint B.V.

As empresas da Unify estão atualmente no processo de integração.

8.5. Gestão de Resposta à Incidente

Os eventos de segurança são abordados pela Atos com relação aos procedimentos operacionais padrão e processos baseados em ferramentas, com base no "ITIL Best Practice", de forma a restaurar a operação sem falhas o mais rápido possível. Os incidentes de segurança são monitorados e analisados imediatamente pela organização Atos Security Management. Dependendo da natureza do evento, as equipes de serviço e especialistas apropriados e necessários participarão do processo, incluindo a "CSIRT" (Computer Security Incident Response Team (equipe de resposta a incidentes de segurança de computadores) da Atos. As empresas da Unify estão atualmente no processo de integração a este Gerenciamento de Respostas a Incidentes.

8.6. Privacidade por Design e Privacidade por Padrão (Art. 25 Seção 2 GDPR)

A proteção de dados na Atos é levada em consideração o mais rapidamente possível através de predefinições favoráveis à proteção de dados ("Privacidade por design e por padrão") para impedir o processamento ilegal ou o uso indevido de dados. A predefinição técnica apropriada destina-se a garantir que apenas os Dados Pessoais realmente necessários para o objetivo específico (Princípio da Minimização de Dados) sejam coletados e processados.

Os Padrões para Privacidade por Design e Privacidade por Padrão são definidos no “Atos Secure Coding Guideline” (Diretriz de Codificação Segura) e no “Atos Secure Coding Policy” (Política de Codificação Segura).

A fim de obter um processamento de dados pessoais de baixo risco, entre outros, as seguintes medidas de proteção estão em vigor:

- Minimize a quantidade dos dados pessoais;

- Pseudo anonimize ou criptografe os dados o mais cedo possível;
- Criar transparência no que diz respeito aos procedimentos e processamento de dados;
- Excluir ou anonimizar dados o mais cedo possível;
- Minimize o acesso aos dados;
- Programe as opções de configuração existentes para os valores mais favoráveis à privacidade;
- Documente a avaliação dos riscos para as pessoas envolvidas.