1. Finalidade

A finalidade desta política é definir os requisitos de privacidade e proteção de dados para cumprir a Política Global de Privacidade da Teleperformance e o apoio ao Programa de Privacidade.

2. Abrangência

São escopo desta política todas as filiais, afiliadas e sites da Teleperformance.

Esta política é aplicável a todos os colaboradores da Teleperformance.

Todas as empresas de Teleperformance devem em primeiro lugar e acima de tudo cumprir as suas leis locais e regulamentos e, em caso de conflito entre as suas leis locais e esta Política, as leis locais devem prevalecer.

3. Definições

Todas as definições são retiradas da **Carta Global de Privacidade e Conformidade** ou das políticas citadas nele, mas estão listados abaixo para facilidade a sua utilização. Em caso de conflito, a definição constante na Carta tem precedência.

Aplicativos significa Sistemas que processam ou armazenam Registros e Informações.

Registros do Cliente significam registros recebidos de um Cliente, os Clientes do cliente, ou gerados por Teleperformance em nome do Cliente.

Demanda Governamental Transfronteiriça significa uma demanda governamental que envolve o envio de dados além das fronteiras ou transferências subsequentes.

Controlador de Dados significa a pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, só ou em conjunto com outros, determina os fins e meios do Processamento de Dados Pessoais.

Processador de Dados significa uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que processa dados pessoais em nome do Controlador.

Titular dos dados significa qualquer pessoa física.

Acordo de Processamento de Dados significa a utilização de modelos aprovados pelo Departamento Global de Privacidade & Conformidade ou redação contratual que esteja de acordo com as orientações do Departamento Global de Privacidade & Conformidade pelo departamento jurídico e define a função da Teleperformance no processamento dos Dados Pessoais, bem como todos os outros elementos exigidos pela legislação de privacidade aplicável.

Autoridade de Proteção de Dados (APD) significa uma autoridade de proteção de dados ou outro organismo regulador ou governamental com responsabilidade estatutária na área de Envolvimento Regulamentar.

Departamento Global de Privacidade & Conformidade significa o Diretor de Privacidade e os Vice-Presidentes Sênior de Privacidade e Conformidade.

Treinamento Global de Privacidade significa o curso de Treinamento Global de Privacidade mantido pelo Departamento Global de Privacidade & Conformidade, para o qual todos os funcionários estão abrangidos. Existem 2 versões: uma para agentes e operacionais e a outra aplicável para o supervisor e acima.

Demanda Governamental significa uma exigência legal emitida válida, intimação, mandado, solicitação de informação, ordem, julgamento ou outra solicitação governamental por qualquer agência, autoridade, corte ou tribunal para Dados Pessoais.

Demanda Governamental Interna significa uma Demanda Governamental de Dados Pessoais (como da Polícia) dentro do mesmo país ou jurisdição de origem dos Dados Pessoais.

Transferência subsequente significa a transferência de Dados Pessoais para outra parte após e uma transferência transfronteiriça.

Dados Pessoais significa qualquer informação relacionada a um Titular de Dados identificado ou identificável. Um titular de dados identificável é aquele que pode ser identificado, direta ou indiretamente, em particular por referência a um identificador, como nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética , mental, econômica, cultural ou social dessa pessoa natural.

Processamento de Risco Potencialmente Alto significa quando o Processamento de Dados Pessoais envolve qualquer um dos seguintes elementos: Avaliação/Pontuação; Tomada de decisão automatizada; Monitoramento Sistemático; Dados Sensíveis; Processamento de Dados em grande escala; Combinação de Conjuntos de Dados; Titulares de Dados Vulneráveis; Nova tecnologia; Impedir que o Titular dos Dados exerça o direito; Transferência transfronteiriça de Dados; ou qualquer outro processamento que possa potencialmente (negativamente) impactar os Titulares dos Dados.

Processo ou **Processamento,** em relação aos Dados Pessoais, significa qualquer operação ou conjunto de operações realizadas sobre os Dados Pessoais ou conjuntos de Dados Pessoais, por meios automáticos ou não, que inclui a coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, difusão ou de outra forma, de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição dos Dados Pessoais.

Registros significam Informações, sejam cópias impressas ou eletrônicas, criadas, recebidas e mantidas como evidência pela Teleperformance, em cumprimento de obrigações legais, conformidade estatutária ou regulamentar ou na transação de negócios.

Envolvimento regulamentar significa gerenciar as interações entre a Teleperformance e a APD, incluindo, sem limitação:

- **Aprovação:** obtenção da aprovação da APD para determinados tipos de atividades de processamento, quando necessário;
- **Nomeação do Encarregado da Proteção de Dados (EPD):** notificar à APD sobre a nomeação de um EPD, um ponto de contato ou outra nomeação obrigatória;
- **Notificação de Incidente:**
  - **Notificação à APD**: garantir que a APD seja notificada dentro do prazo legal exigido de quaisquer incidentes de dados, quando necessário;
  - **Notificação ao Titular dos Dados:** notificar os Titulares dos Dados sobre o incidente de dados, quando necessário;
- **Tratamento de Investigações:** responder dentro dos prazos legais às solicitações de informações ou investigações da APD;
- **Notificação:** notificar à APD sobre os tipos de atividades de processamento de dados realizadas;
- **Registro:** registro de subsidiárias ou afiliadas na APD como controladores ou processadores de dados.

Sub-processador significa uma Empresa TP contratada por outra Empresa TP ou Terceiros, atuando como Processador de Dados, para processar Dados Pessoais.

Comitê de Tecnologia, Privacidade e Segurança significa o órgão da Teleperformance que serve para revisar as Solicitações e processos propostos para quaisquer questões de privacidade, segurança e proteção de dados e fornecer orientação para mitigar tais questões.

Teleperformance ou **Empresa (s) TP** significa qualquer / toda(s) as filial(is) do Grupo.

GRT significa Gestão de Risco de Terceiros.

Política GRT significa a política que define a abordagem e governança necessária para o Programa de Gestão de Risco de Terceiros.

Terceiros GRT significa uma entidade, incluindo uma filial, que tenha uma relação comercial com uma Empresa TP ou os seus clientes, e que não seja ela própria um cliente da TP . As relações com terceiros incluem tanto os **fornecedores** como os **não fornecedores.**

• **Fornecedores** os terceiros são prestadores de serviços/fornecedores que proveem um produto ou serviço a uma empresa TP. Esses relacionamentos são obtidos por meio de Compras Global ou do processo de suprimento/compras local. O pagamento normalmente é feito por contas a pagar.

• **Nao fornecedores** relacionamentos com terceiros não fornecedores são normalmente adquiridos por uma linha / segmento de negócios diretamente, e não por meio da função de compras. A remuneração financeira, se aplicável, é normalmente prestada fora dos processos de contas a pagar. Esses relacionamentos com terceiros podem ser administrados exclusivamente por uma linha/segmento de negócios ou em conjunto com uma função corporativa de gerenciamento de risco de terceiros. Exemplos de **não fornecedores** incluem instituições de caridade, joint ventures, agentes, membros afins e associações comerciais.

Risco de Terceiros GRT significa os riscos potenciais que surgem ao lidar com Terceiros GRT, incluindo: Incumplimento com a Legislação Aplicável, Cyber/InfoSec, Privacidade, Segurança Física, Continuidade de Negócios, País, Viabilidade Financeira, Reputação, Tecnologia/ Inovação.

Conforme definido na “Política de Privacidade de Dados do Grupo Teleperformance - Interna”

• **Cliente**

Conforme definido no "Procedimento de Registros de Processamento"

• **Atividades de Tratamento de Dados / ATD**

4. Política de Privacidade e Proteção de Dados

1. Registros de Processamento

1.1. Criação e Manutenção de Registros de Processamento

Teleperformance deve criar e manter Registros escritos de todo Processamento de Dados Pessoais (conhecidos como Registros de Processamento). Isso se aplica quando Teleperformance atua como Controlador de Dados ou Processador de Dados.

Os Registros de Processamento devem ser mantidos de acordo com o Procedimento de Registros de Processamento.

Os Registros de Processamento devem conter informações determinadas pelos requisitos aprovados do Departamanto Global de Privacidade & Conformidade, conforme definido pelos modelos (avaliação) aprovados. Os Registros de Processamento devem incluir:

- Atividades de processamento de negócios que incluam Processamento de Dados Pessoais.
- Sistemas de TI que incluam Processamento de Dados Pessoais.

1.2. Revisão de Registros de Processamento

Os Registros de Processamento devem ser revisados periodicamente de acordo com os requisitos mínimos do Departamento Global de Privacidade & Conformidade (pelo menos semestralmente).

As revisões e os resultados das revisões devem ser documentados.

1.3. Solicitações de Acesso das Autoridades de Proteção de Dados

Os Registros de Processamento devem ser compartilhadas com as Autoridades de Proteção de Dados se forem feitas solicitações oficiais (por exemplo, em caso de uma auditoria ou violação de dados), ou se forem exigidos pelas regulamentações de privacidade.

Os Registros de Processamento só devem ser compartilhados com as Autoridades de Proteção de Dados se o Departamento Global de Privacidade & Conformidade tiver fornecido a sua aprovação.

2. Direitos do Titular de Dados

2.1. Compreensão e Documentação dos Direitos do Titular de Dados

Os Titulares dos Dados podem ter direitos legais relacionados aos seus Dados Pessoais e os direitos legais específicos variam de acordo com as regulamentações de privacidade locais. O Departamento Global de Privacidade & Conformidade fornece orientação central sobre os direitos aplicáveis.

2.2. Responder às Solicitações de Direitos de Ttitulares de Dados

Quando a Teleperformance for o Processador de Dados de Clientes que são os Controladores de Dados, a Teleperformance deve aderir a quaisquer requisitos contratuais do Cliente e, em qualquer caso, notificar o Cliente sem demora quando receber uma solicitação de Direitos do Titular de Dados (DTD) e fornecer cooperação razoável em resposta ao mesmo.

Quando a Telepeformance é o Controlador de Dados, as solicitações de Direitos do Titular de Dados (DTD) devem ser honradas de acordo com os requisitos da regulamentação de privacidade local e de acordo com o processo aprovado do Departamento Global de Privacidade & Conformidade:

1. A Teleperformance deve fornecer uma ferramenta e processo de DTD aprovado pelo Departamento Global de Privacidade & Conformidade que permita que os Titulares de Dados enviem uma Solicitação de Direitos do Titular de Dados. Se uma solicitação de DTD válida for feita fora da ferramenta, a Teleperformance deve inserir essas solicitações na ferramenta de DTD usando o recurso “Em Nome de” dentro de 48 horas. Exemplos de recebimento de uma solicitação DTD incluem, mas não estão limitados a:

a. Receber uma solicitação por e-mail.
b. Receber uma solicitação por carta.
c. Um gerente de departamento ou RH recebe uma solicitação verbal.
d. Receber uma solicitação via formulário da web.

2. As solicitações de DTD devem ser atendidas e acompanhadas pela Teleperformance em tempo hábil de acordo com os requisitos de regulamentação de privacidade relevantes e o processo de DTD gerenciado e aprovado pelo Departamento Global de Privacidade & Conformidade.

3. Todos os departamentos relevantes (por exemplo, RH, TI, gestão) devem colaborar para honrar as solicitações de DTD de acordo com os requisitos do Departamento Global de Privacidade & Conformidade e regulamentos de privacidade relevantes. Exemplos de cooperação necessária incluem, mas não se limitam a:

a. O departamento de TI exclui registros de Dados Pessoais mediante solicitação.
b. O departamento de Marketing, garante que os *opt-outs* do marketing sejam cumpridos.
c. O departamento de RH analisa localizações de Dados Pessoais (por exemplo, aplicativos, unidades compartilhadas, etc.).
d. Gestão fornecendo recursos e suporte suficientes.

2.3. Respondendo as consultas da APD relacionadas ao DTD

Caso as solicitações de Direitos do Titular de Dados sejam escaladas para uma APD, deve ser prestada total cooperação de acordo com as instruções do Departamento Global de Privacidade & Conformidade.

3. Requisitos Contratuais do Processamento de Dados Pessoais do Cliente

3.1. Garantindo Requisitos Contratuais Relevantes do Cliente

Os contratos entre a Teleperformance e os Clientes da Teleperformance devem conter Acordos de Processamento de Dados que descrevem o Processamento de Dados Pessoais que a Teleperformance deve realizar sob instrução do Cliente, incluindo transferências (internacionais) de Dados Pessoais.

Cada Linha de Negócios (LN) separada ou distinta ou Atividade de Tratamento de Dados deve ser coberta por um Acordo de Processamento de Dados (ou instrução semelhante).

3.2. Alterações no Processamento de Dados Pessoais Relacionado ao Cliente

Em caso de alterações no Processamento de Dados Pessoais relacionado ao Cliente, o Cliente deve fornecer instruções formais atualizadas que a Teleperformance deve seguir. A instrução formal deve consistir em um Acordo de Processamento de Dados atualizado ou um método de instrução contratualmente reconhecido.

3.3. Processamento de Dados Pessoais sem Instrução do Cliente

A Teleperformance só deve realizar o Processamento de Dados Pessoais de acordo e em conformidade com as instruções formais (por exemplo, um Acordo de Processamento de Dados). Se tais instruções não forem fornecidas, a Teleperformance não deve realizar o Processamento de Dados Pessoais em nome de um Cliente.

3.4. Instruções de infracção

A Teleperformance deverá informar o cliente, se na sua opinião, uma Instrução de Processamento infringir a legislação e/ou regulamentos aplicáveis.

Qualquer infracção identificada deve ser notificada ao Departamento Global de Privacidade & Conformidade.

4. Base Legal de Processamento

4.1. Compreensão e Documentação da Base Legal de Processamento

A Teleperformance deve compreender e documentar sua base legal de Processamento de Dados Pessoais de acordo com as orientações do Departamento Global de Privacidade & Conformidade. A base legal do Processamento varia de acordo com os regulamentos de privacidade relevantes e aplicáveis.

4.2. Somente execute Processamento de Dados Pessoais com Base Legal Válida

Todo Processamento de Dados Pessoais deve ter uma base legal válida de processamento, caso contrário, não deve ser realizado.

4.3. Processe Dados Pessoais apenas para os Fins para os quais foram Coletados

Os Dados Pessoais devem ser processados apenas para os fins para os quais foram coletados. O Processamento Adicional não deve ocorrer para fins incompatíveis com a coleta original. O Departamento Global de Privacidade & Conformidade deve ser consultado sempre que houver qualquer dúvida sobre a compatibilidade com o propósito original.

5. Aviso e Consentimento

5.1. Emissão de Avisos de Privacidade e Obtenção de Consentimento

Todos os Titulares de Dados da Teleperformance (por exemplo, candidatos, funcionários, contratados, usuários de aplicativos de propriedade da Teleperformance onde ocorrem níveis significativos de Dados Pessoais ou processamento analítico), devem receber um aviso de privacidade explicando os detalhes do Processamento de Dados Pessoais realizado pela Teleperformance, a base legal do Processamento, os direitos do Titular de Dados e detalhes de contato da Teleperformance. Quando a base legal do Processamento for o consentimento, este deve ser obtido em termos claros e de acordo com a lei aplicável.

O aviso de privacidade e documentos de consentimento utilizados (por exemplo, o conteúdo do aviso de privacidade e consentimento) e quaisquer alterações significativas devem ser aprovados pelo Departamento Global de Privacidade & Conformidade antes do uso e revisados anualmente.

5.2. Documentação de Aviso de Privacidade e Consentimento de Uso

As atividades e resultados do aviso sobre privacidade e consentimento devem ser documentados e acessíveis ao Departamento Global de Privacidade & Conformidade

5.3. Revogação do Consentimento

Quando exigido pelos regulamentos de privacidade relevantes e nos casos em que o consentimento for dado pelo Titular dos Dados para o Processamento de Dados Pessoais, o Titular de Dados deve poder revogar o consentimento com a mesma facilidade com que foi dado, e isso não deve resultar em consequências negativas para o Titular de Dados.

6. Terceiros GRT e Sub-processadores

6.1. Garantindo Requisitos Contratuais Relevantes de Terceiros GRT e Sub-processadores

Todos os Terceiros GRT e Sub-processadores usados pela Teleperformance devem ter um contrato cobrindo todos os serviços prestados.

Os contratos entre Teleperformance e Terceiros GRT e Sub-processadores da Teleperformance devem conter Acordos de Processamento de Dados que descrevem o Processamento de Dados Pessoais que terceiros e Sub-processadores devem realizar em nome da Teleperformance, incluindo transferências (internacionais) de Dados Pessoais.

O Acordo de Processamento de Dados usado deve ser baseado em um modelo aprovado pelo Departamento Global de Privacidade & Conformidade.

6.2. Alterações no Processamento de Dados Pessoais relacionados a Terceiros GRT e Sub-processadores

Em caso de alterações no Processamento de Dados Pessoais de Terceiros GRT ou Sub-processadores , o Acordo de Processamento de Dados deve ser atualizado.

6.3. *Due Diligence* de Terceiros GRT e Sub-Processadores

A *due diligence* baseada em risco deve ser realizada em todos os terceiros e Sub-processadores periodicamente de acordo com os requisitos do Departamento Global de Privacidade & Conformidade e utilizando os questionários/modelos de *due diligence* aprovados.

6.4. Aprovação do Cliente para uso de Sub-processador

No caso de um Sub-processador seja utilizado para um Cliente (que realiza parte do trabalho que a Teleperformance foi contratada para realizar em nome de um Cliente), o Cliente deve ser informado e fornecer aprovação formal para seu uso. A aprovação pode ser específica para um Sub-processador em particular ou geral para um tipo de Sub-processador (por exemplo, afiliados da Teleperformance). A aprovação deve ser documentada.

7. Política Global de Retenção de Dados

7.1. Aplicação de Códigos de Retenção de Registros

A Política Global de Retenção de Dados deve ser cumprida.

Todos os Sistemas nos quais os Registros são armazenados devem ser listados no Registro Global de Software (RGS) e as perguntas necessárias sobre Gerenciamento de Registros do RGS devem ser preenchidas, incluindo a listagem dos Códigos de Retenção de Registros e Códigos de Classificação de Informações aplicáveis.

Todos os locais onde os registros impressos são armazenados devem ser identificados e os registros devem ser armazenados de acordo com os Códigos de Retenção de Registros e Códigos de Classificação de Informações aplicáveis.

7.2. Requisitos para Devolução ou Destruição de Registos de Clientes

Todos os sistemas e locais nos quais os Registros do Cliente são armazenados devem ser identificados e aplicado o código de Retenção de Registro CLS100.

Todos os Registros do Cliente devem ser devolvidos ou destruídos de acordo com acordos contratuais, ou no prazo de 90 dias da rescisão dos serviços (por exemplo, rescisão de todos os serviços para um cliente ou rescisão dos serviços para uma Linha de Negócios específica).

Qualquer desvio deve ter uma aprovação de exceção de um ´Vice-presidente Sênior de Privacidade´.

A devolução ou destruição dos Registros do Cliente (ou não, devido a uma exceção aprovada) deve ser documentada de acordo com a Política Global de Retenção de Dados.

7.3. Retenção de Dados do Controlador de Dados Pessoais

Os Dados Pessoais mantidos pela Teleperformance, em que a Teleperformance é o Controlador de Dados (por exemplo, dados de candidatos, funcionários ou ex-funcionários), só devem ser mantidos apenas pelo tempo necessário e de acordo com os Períodos de Retenção de Registros. Uma vez que os Dados Pessoais não sejam mais necessários, devem ser destruídos com segurança ou tornados anônimos. Quando os dados pessoais se tornarem anônimos, deverá ser feito de forma aprovada pelo Departamento Global de Privacidade.

8. Avaliações de Privacidade, Avaliações de Impacto de Proteção de Dados e o Comitê de Privacidade e Segurança de Tecnologia

8.1. Comitê de Privacidade e Segurança de Tecnologia

As Avaliações de Privacidade e Avaliações de Impacto de Proteção de Dados (AIPDs) devem ser conduzidas dentro da governança do Comitê de Privacidade e Segurança de Tecnologia (TPSC), por meio do qual as ações, alterações e projetos significativos de Processamento de Dados Pessoais /compartilhamento de dados são avaliados a partir de uma perpectiva de privacidade e segurança.

As seguintes sub-seções (9.2 a 9.6) referem-se aos requisitos relacionados à privacidade (e não aos requisitos relacionados à segurança).

8.2. Requisitos para iniciar uma Avaliação de Privacidade

Deve ser realizada uma Avaliação de Privacidade quando existe Processamento de Risco Potencialmente Elevado ou quando exigido por leis/regulamentos relevantes.

Exemplos não exaustivos de mudanças ou projetos relevantes que estão no escopo das Avaliações de Privacidade:

- Utilização de uma nova ferramenta de RH baseada em SaaS.
- Terceirização de processos relacionados à pensão ou saúde para um prestador de serviços.
- Mudança de infraestrutura local para infraestrutura baseada em nuvem.
- Mudança baseada em processos relacionados com o processamento de Dados Pessoais de RH.
- Utilização de Dados Pessoais de maneiras inicialmente (e no ponto de coleta) não intencionais.
- Realização de novos tipos de analítica ou análise de Dados Pessoais.
- Fornecimento ou compartilhamento de Dados Pessoais a terceiros sem um contrato legalmente vinculativo (incluindo um Acordo de Processamento de Dados).
- Utilização de nova tecnologia bot para fornecer melhor atendimento ao cliente.
- Início de um projeto para fornecer melhor monitoramento e análise do trabalho do agente.

Em caso de dúvida quanto à necessidade de uma Avaliação de Privacidade, o Departamento Global de Privacidade & Conformidade deve ser contatado e sua avaliação (quanto à necessidade ou não de uma Avaliação de Privacidade) é vinculativa.

8.3. Quando uma Avaliação de Privacidade deve ser iniciada

Uma Avaliação de Privacidade deve ser iniciada o mais rápido possível no ciclo de vida de desenvolvimento de mudança ou projeto (de preferência no início dele). Isso permitirá que possíveis requisitos de privacidade e retificações sejam feitos o mais rápido possível e reduzirá os custos.

8.4. Requisitos de Avaliação de Privacidade

Uma Avaliação de Privacidade deve ser baseada na metodologia aprovada pelo Departamento Global de Privacidade & Conformidade. Isso consiste em usar a versão mais recente do formulário TPSC aprovado.

O avaliador do Departamento Global de Privacidade & Conformidade pode ter perguntas adicionais sobre a mudança ou projeto, e essas perguntas devem ser respondidas de forma satisfatória para o avaliador do Departamento Global de Privacidade & Conformidade. As Avaliações de Privacidade devem ser documentadas.

8.5. Aprovação da Avaliação de Privacidade

Para que uma Avaliação de Privacidade seja aprovada, ela deve ter a aprovação do responsável do Departamento Global de Privacidade & Conformidade e do Comité de Privacidade e Segurança Tecnológica (TPSC), quando necessário.

8.6. Avaliação de Impacto de Proteção de Dados (AIPD)

Se o Regulamento Geral de Proteção de Dados (RGPD) da UE for aplicável e uma Avaliação de Privacidade mostrar que o processamento provavelmente resultará em um alto risco para os indivíduos, deve ser realizada uma Avaliação de Impacto de Proteção de Dados (AIPD) em conjunto com o Departamento Global de Privacidade & Conformidade.

Se uma Avaliação de Impacto de Proteção de Dados resultar em riscos elevados permanentes para os direitos e liberdades dos indivíduos que não possam ser mitigados, a APD da UE / EEE pertinente deve ser consultada antes que a alteração ou o projeto possa ser implementado (e os Dados Pessoais correspondentes possam ser processados).

9. Envolvimento regulamentar com APDs

Todo envolvimento regulamentar com uma APD deve ser aprovado com antecedência pelo Departamento Global de Privacidade & Conformidade. O Departamento Global de Privacidade & Conformidade pode realizar o Envolvimento Regulamentar por conta própria ou fornecer autoridade delegada por escrito para que seja realizado pelo Líder de Privacidade do País ou EPDs Locais.

9.1. Aprovação da APD

Se as atividades de processamento de Dados Pessoais exigirem a aprovação de uma APD, a Teleperformance deverá obter a aprovação da APD antes de realizar o Processamento de Dados Pessoais.

9.2. Nomeação do Encarregado de Proteção de Dados (EPD):

A nomeação de um EPD, ponto de contato ou outra pessoa necessária deve ser aprovada pelo Departamento Global de Privacidade & Conformidade. A APD deve ser notificada de tal nomeação pela Teleperformance quando necessário.

9.3. Notificação de Incidente:

9.3.1. Notificação à APD:

A Equipe de Resposta a Incidentes Globais (GIRT) deve documentar e rastrear o número de incidentes de dados confirmados através da Teleperformance e quaisquer notificações a uma APD.

O Departamento Global de Privacidade & Conformidade deve garantir que a APD seja notificada dentro do prazo legal exigido de quaisquer incidentes de dados, quando necessário.

9.3.2. Notificação ao Titular de Dados:

A GIRT documentará e rastreará quaisquer notificações feitas aos Titulares de Dados sobre incidentes de dados.

O Departamento Global de Privacidade & Conformidade deve garantir que os Titulares de Dados sejam notificados dentro do prazo legal exigido de quaisquer incidentes de dados, quando necessário.

9.4. Tratamento da Investigação

Qualquer Investigação Regulatória por uma APD deve ser respondida dentro do prazo exigido. Quando necessário, o Líder de Privacidade do País pertinente deverá entrar em contato e fornecer suporte ao Departamento Global de Privacidade & Conformidade no preenchimento e envio da resposta.

9.5. Notificação

Se as atividades de processamento de Dados Pessoais exigirem a aprovação de uma APD, a Teleperformance deverá obter a aprovação da APD antes de realizar o Processamento de Dados Pessoais.

9.6. Registro

Quando necessário a Teleperformance deverá registrar suas subsidiárias/filiais junto às Autoridades de Proteção de Dados pertinente como Controlador de Dados ou Processador de Dados, conforme aplicável.

10. Demandas Governamentais de Dados Pessoais

As solicitações de Dados Pessoais sobre Titulares de Dados provenientes da aplicação da lei, agências governamentais e outros órgãos reguladores ("Demandas Governamentais") devem ser tratadas de acordo com os requisitos descritos no documento **"Procedimento da Teleperformance para Transferências de Dados Pessoais exigidas por uma Demanda Governamental"** (o **"Procedimento"**).
Quando um funcionário da Teleperformance recebe uma Demanda Governamental, esta deve ser enviada no mesmo dia em que é recebida para: o Líder de Privacidade do País e Departamento Jurídico para Demandas Governamentais do País (a menos que uma Exceção se aplique ao Procedimento); e Privacidade Global e Diretor Jurídico Regional para Demandas Governamentais Transfronteiriças.

O Departamento de Privacidade Global e o Departamento Jurídico são responsáveis pelo cumprimento do Procedimento e pela manutenção de registros das Demandas Governamentais.

11. Avaliação de Risco de Privacidade

Cada departamento global e/ou regional e cada filial operacional e/ou grupo de filiais operacionais deve realizar uma Avaliação de Risco de Privacidade de acordo com os requisitos do Departamento Global de Privacidade & Conformidade. A Avaliação de Risco de Privacidade deve ser revisada pelo menos uma vez por ano ou quando houver uma mudança significativa. As revisões e quaisquer alterações serão apoiadas por meio do Departamento Global de Privacidade & Conformidade e do Líder de Privacidade do País.

12. Leis de Privacidade Locais

Todos os locais da Teleperformance devem manter um registro atualizado e preciso das leis e regulamentos aplicáveis aos negócios relativos à privacidade, isso será apoiado pelo Departamento Global de Privacidade & Conformidade e pelo Líder de Privacidade do Pais.

O Líder de Privacidade do País deve usar a Orientação de Dados regularmente para pesquisar e identificar as obrigações relevantes relacionadas ao Envolvimento Regulamentar. O Departamento Global de Privacy & Conformidade deve manter um rastreador que identifique as obrigações do Envolvimento Regulamentar para cada país, o qual será mantido atualizado e preciso.

13. Dados de Saúde (HIPAA)

O Anexo A define os requisitos de como a Teleperformance deve usar, divulgar e proteger as informações de acordo com a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) sempre que qualquer empresa dentro da família de entidades Teleperformance utilize Informações de Saúde Protegidas (ISP) ou Informações eletrônicas de Saúde Protegidas (eISP).

14. Volume de Processamento de Dados

A Teleperformance é obrigada a manter uma visão geral do volume de dados pessoais processados em nossa função como Controlador e Processador. Cada departamento global e/ou regional e cada filial operacional e/ou grupo de filiais operacionais deve fornecer as informações necessárias de acordo com as instruções do Departamento Global de Privacidade & Conformidade.

15. Responsabilidades e Autoridades

Cargo	Responsabilidade	Autoridade
Todos	Garantir o cumprimento de toda a legislação e regulamentação aplicável	Todos
Gerencia; Coordenação e Supervisão	A capacidade de respondermos a pedidos das autoridades de controle; a administração processos judiciais e administrativos; detectar e prevenir fraude; e, realizar nossas atividades comerciais.	Operação e Time de Prevenção a Fraude
Gerencia de Privacidade de Dados	Manter um registro atualizado e preciso das leis e regulamentos aplicáveis aos negócios relativos à privacidade, isso será apoiado pelo Departamento Global de Privacidade & Conformidade e pelo Líder de Privacidade do Pais.	Jurídico

16. Classificação do Documento

Uso Interno.

Anexo A

Lei de Portabilidade e Responsabilidade de Seguro Saúde de 1996 (HIPAA)

Objetivo

O objetivo do Anexo A é complementar os requisitos contidos no TISPS 18 e definir os requisitos de como a Teleperformance deve usar, divulgar e proteger as informações de acordo com a Lei de Responsabilidade e Portabilidade de Seguro de Saúde (HIPAA).

Na Teleperformance, levamos muito a sério as nossas responsabilidades em relação à confidencialidade do cliente e do paciente e dedicamos tempo e recursos para treinar nossa força de trabalho e desenvolver e implementar todos os componentes de nosso Programa de Conformidade HIPAA.

Escopo

O Anexo A deve ser usado pela Teleperformance sempre que qualquer empresa da família de entidades Teleperformance utilize Informações de Saúde Protegidas (ISP) ou Informações eletrônicas de Saúde Protegidas (eISP).

Definições

Notificação de Infração significa que as entidades cobertas devem notificar os indivíduos afetados, o HHS e, em alguns casos, a mídia sobre uma violação de ISP não seguro. Uma infração é um uso ou divulgação nao permitida sob a Regra de Privacidade que compromete a segurança ou privacidade de informações de saúde protegidas (ISP).

Associado Comercial significa uma pessoa ou organização, que não seja membro da força de trabalho de uma entidade coberta, que desempenha determinadas funções em nome de, ou fornece determinados serviços a, uma entidade coberta que envolve acesso a ISP.

Contrato de Associação Comercial (Contrato AC) significa um contrato formal por escrito entre a Teleperformance e uma Entidade Coberta que exige que a Teleperformance cumpra requisitos específicos relacionados a ISP.

Entidade Coberta significa um plano de saúde, provedor de saúde ou centro de coordenação de saúde que deve cumprir a Regra de Privacidade da HIPAA.

Informação Não Identificada significa informação sobre saúde que não identifica um indivíduo e em relação à qual não existe base razoável para acreditar que a informação possa ser utilizada para identificar um indivíduo.

Divulgação significa, para informações que são informações de saúde protegidas (ISP), qualquer liberação, transferência, fornecimento de acesso ou divulgação de qualquer outra forma de informações de saúde individualmente identificáveis para pessoas não empregadas ou trabalhando na Teleperformance com uma necessidade comercial de conhecimento da ISP.

eISP significa qualquer informação de saúde protegida (ISP) que é coberta pela Lei de Responsabilidade e Portabilidade de Seguro de Saúde de 1996 (HIPAA) e é produzida, salva, transferida ou recebida em formato eletrônico.

Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) e Lei de Tecnologia da Informação em Saúde para Saúde Econômica e Clínica (HITECH) significam políticas, procedimentos e processos que são exigidos para empresas que armazenam, processam ou lidam com informações eletrônicas de saúde protegidas (eISP).

Mínimo Necessário significa que apenas deve acessar, utilizar ou divulgar a quantidade mínima de Informações de Saúde Protegidas necessárias para cumprir a finalidade pretendida de acesso, uso ou divulgação.

Regra de Privacidade significa que as circunstâncias em que as informações de saúde protegidas de um indivíduo podem ser usadas ou divulgadas por entidades cobertas serão definidas e limitadas. Uma entidade coberta não pode usar ou divulgar informações protegidas de saúde, exceto: (a) conforme a Regra de Privacidade permite ou exige; ou (b) conforme o indivíduo que é o titular das informações (ou o representante pessoal do indivíduo) o autorize por escrito.

Informação de Saúde Protegida (ISP) significa toda "informação de saúde individualmente identificável" que é transmitida ou mantida em qualquer forma ou meio por uma Entidade Coberta. Informação de saúde individualmente identificável é qualquer informação que possa ser utilizada para identificar um indivíduo e que foi criada, utilizada ou divulgada (a) durante a prestação de um serviço de saúde, como diagnóstico ou tratamento, ou (b) em relação ao pagamento pela prestação de serviços de saúde. Sempre que este documento utilize a sigla "ISP", também inclui o termo "eISP".

Regra de Segurança significa que as Entidades Cobertas devem manter salvaguardas administrativas, técnicas e físicas razoáveis e apropriadas para proteger as informações eletrônicas de saúde protegidas (eISP).

Uso significa o compartilhamento, emprego, aplicação, utilização, exame ou análise de informações de saúde individualmente identificáveis por qualquer pessoa que trabalhe para ou dentro da Empresa, ou por um Associado Comercial da Empresa.

1. Liderança em Segurança e Privacidade ao tratar com Informações de Saúde Protegidas

Teleperformance deve ter um Responsável pela Conformidade de Privacidade e Segurança HIPAA para supervisionar o desenvolvimento, implementação, manutenção e adesão às políticas e procedimentos de privacidade relativos ao uso seguro e tratamento de ISP em conformidade com a HIPAA. Esta função deve fazer parte da Equipe de Segurança e Privacidade da Teleperformance, que inclui:

a. Departamento Global de Segurança da Informação
b. Departamento Global de Auditoria e Conformidade
c. Departamento Global de Privacidade e Conformidade
d. Equipe Global de Resposta a Incidentes

1.1 Papel e Responsabilidades do Responsável pela Conformidade de Privacidade e Segurança HIPAA da Teleperformance

O Responsável de Conformidade de Privacidade e Segurança HIPAA supervisiona o desenvolvimento, implementação, manutenção e adesão às políticas e procedimentos de privacidade e segurança relativos ao uso seguro e tratamento de informações de saúde protegidas (ISP) em conformidade com as leis e regulamentos federais e estaduais semelhantes relacionados ao HIPAA.

As responsabilidades do Responsável de Conformidade de Privacidade e Segurança HIPAA incluem:

- Monitorar o desenvolvimento, implementação e melhoria de políticas e procedimentos relativos ao HIPAA.
- Implementar políticas e procedimentos para estender a obrigação de confidencialidade e treinamento de privacidade HIPAA em todas as partes relevantes dos funcionários da Teleperformance.
- Implementar e manter políticas e procedimentos de segurança para proteger a confidencialidade, integridade e acessibilidade das ISP.

2. Usos e divulgações permitidos de Informações de Saúde Protegidas (ISP)

Teleperformance usará e divulgará ISP somente conforme permitido pela HIPAA. É política da Teleperformance estar em total conformidade com a HIPAA. Todos os funcionários com acesso a ISP devem cumprir os usos e divulgações permitidos de ISP.

2.1 Usos de ISP pela Teleperformance

A Teleperformance só poderá utilizar ISP para nosso gerenciamento, administração, agregação de dados e obrigações legais na medida em que tal uso de ISP seja permitido ou exigido por um Contrato AC. Podemos usar ou divulgar ISP em nome de, ou para fornecer serviços a Entidades Cobertas para fins de cumprimento de nossas obrigações de serviço com elas, somente se tal uso ou divulgação das ISP for permitido ou exigido pelo Contrato AC e não violar a HIPAA.

Caso as ISP deva ser divulgada a um subcontratado ou agente, a Teleperformance firmará contratos nos quais esse subcontratado ou agente concorda em obedecer as mesmas restrições e condições que se aplicam à Teleperformance nos termos do Contrato AC, incluindo a implementação de salvaguardas razoáveis e adequadas.

A Teleperformance poderá também divulgar as ISP para reguladores governamentais quando exigido pela HIPAA.

A Teleperformance poderá utilizar também as ISP para relatar violações da lei às autoridades federais e estaduais competentes.

2.2 Divulgação de ISP de acordo com uma autorização

As ISP podem ser divulgadas para qualquer finalidade se uma autorização que satisfaça todos os requisitos da HIPAA para uma autorização válida for fornecida pelo indivíduo a quem ela pertence. Todos os usos e divulgações feitos de acordo com uma autorização assinada devem ser consistentes com os termos e condições da autorização.

2.3. A Norma 'Mínimo Necessário'

Quando a ISP é usada, divulgada ou solicitado, a HIPAA exige que a quantidade divulgada geralmente deve ser limitado ao 'Mínimo Necessário' para cumprir os objetivos de uso, divulgação ou solicitação. A violação desta política também é uma violação do Manual do Funcionário da Teleperformance.

2.3.1 Mínimo Necessário ao divulgar ISP

Ao fazer divulgações de ISP a qualquer Associado Comercial, Entidades Cobertas ou para fins de auditoria interna/externa, apenas será divulgada quantidade de informação Mínima Necessária.

2.3.2 Mínimo Necessário ao solicitar ISP

Para fazer solicitações de divulgação de ISP de Associados Comerciais, Entidades Cobertas ou indivíduos, apenas será solicitada a quantidade de informação Mínima Necessária.

2.4 Divulgações de ISP para Associados Comerciais

Teleperformance pode divulgar ISP para Associados Comerciais da Teleperformance e permitir que os Associados Comerciais da Teleperformance criem ou recebam ISP em seu nome. No entanto, antes de fazer isso, a Teleperformance deverá primeiro obter garantias de que tal Associado Comercial cumprirá com termos substancialmente semelhantes aos termos de um Contrato AC entre a Teleperformance e uma Entidade Coberta relevante, incluindo disposições para proteger apropriadamente as ISP. Antes de compartilhar ISP com Associados Comerciais, a Teleperformance deve verificar se existe um Contrato AC entre a Teleperformance e o Associado Comercial.

2.5 Divulgações de ISP para Indivíduos

As pessoas têm o direito de acessar, alterar e obter cópias de suas ISP que a Teleperformance ou os Associados Comerciais da Teleperformance mantêm, de acordo com a HIPAA. Quando a Teleperformance receber um pedido para exercer esses direitos, deverá comunicar à Entidade Coberta apropriada para obter instruções antes de responder a tal pedido. A Teleperformance deverá agir de acordo com as instruções da Entidade Coberta.

2.6 Resposta a Incidentes

Ao descobrir um incidente de dados em relação a ISP nao seguro - ou quando exigido por um Contrato AC ou outro acordo entre uma Entidade Coberta e a Teleperformance - a Teleperformance notificará a Entidade Coberta de tal incidente de dados.

A Teleperformance seguirá todas as diretrizes para relatórios de incidentes de dados de acordo com o estabelecido em um Contrato AC, conforme instruído pela Entidade Coberta e a 45 CFR § 164.410.

2.7 Aplicação

O Responsável pela Conformidade de Privacidade e Segurança HIPAA supervisionará o desenvolvimento de regras e sanções quando os funcionários da Teleperformance violarem os requisitos do programa de conformidade HIPAA da Teleperformance.

3. Treinamento Obrigatório de Conscientização sobre Privacidade e Segurança

A Teleperformance fornecerá treinamento de privacidade e segurança HIPAA a todos os membros de sua força de trabalho que usam, acessam, recebem ou solicitam ISP.

O treinamento HIPAA será fornecido a cada novo membro da força de trabalho no prazo de 90 dias após o ingresso da pessoa na Teleperformance.

As mudanças relevantes nas regras e regulamentos da HIPAA serão incorporadas aos materiais de treinamento dentro de um período razoável após a entrada em vigor da alteração.

Os funcionários também farão um treinamento de reciclagem anual que deve incluir os seguintes tópicos:

- Identificando as ISP
- A regra do Mínimo Necessário
- Regras sobre quando e como as ISP podem ser divulgadas
- Importância da confidencialidade
- A necessidade de manter uma contabilidade das divulgações
- Protegendo as ISP ao usar, solicitar, receber ou divulgar ISP
- Identificação de solicitações de privacidade
- Consequências do não cumprimento da Regra de Privacidade da HIPAA

3.1 Manutenção de registros

Todos os registros serão rastreados no myTP, que mantém registros durante todo o seu ciclo de vida para todos os funcionários. Relatórios semanais serão fornecidos aos líderes locais e soluções de clientes para adesão.