Política Global de Privacidade & Proteção de Dados da Ipsos

(em vigor a partir de 25 de maio de 2018)*[1]

---

[1] *Tradução para o Português em 16/12/2020

Política Global de Privacidade & Proteção de Dados da Ipsos

Conteúdo

1. Introdução

Como parte de sua responsabilidade social, a Ipsos está comprometida com a observância internacional de leis, regulamentos e regras de proteção de dados. Esta política de privacidade & proteção de dados ("**Política**" ou "**Política de Proteção de Dados**") aplica-se globalmente ao Grupo Ipsos e é baseada em princípios básicos aceitos mundialmente em relação à proteção de dados. Esta Política adota os princípios fundamentais do Regulamento Geral Sobre a Proteção de Dados *(General Data Protection Regulation "GDPR")* da União Europeia como o padrão mínimo ao qual o Grupo Ipsos, seus funcionários e fornecedores devem aderir.

A Ipsos depende da coleta e da análise de informações a respeito de pessoas vivas ("**Titulares de Dados**") a fim de realizar pesquisas de mercado e negócios associados. Manter a confiança dos respondentes e do público exige que os respondentes não sofram consequências adversas, riscos ou prejuízos diretos como resultado de fornecer à Ipsos suas informações ou seus Dados Pessoais (para obter uma definição e explicação deste termo e outros termos grafados com inicial maiúscula, favor consultar o Glossário), os quais são tratados para os fins comerciais da Ipsos. As informações podem ser obtidas de qualquer tipo de indivíduo ou organização.

Para conduzir seus negócios, a Ipsos também precisa coletar e processar certos tipos de informações a respeito das pessoas com as quais a Ipsos lida. Isto pode incluir atuais, passados ou futuros empregados,, fornecedores e clientes, bem como outras pessoas com as quais ela possa se comunicar. Além disto, a Ipsos pode, ocasionalmente, ser obrigada por lei a tratar certos tipos de Dados Pessoais a fim de cumprir determinadas obrigações legais.

Esta Política descreve os padrões mínimos de como os Dados Pessoais devem ser tratados, coletados, processados e armazenados a fim de cumprir os padrões de proteção de dados da Ipsos.

Usuários de Dados são obrigados a cumprir esta Política ao tratar Dados Pessoais em nome da Ipsos. Qualquer violação a esta Política pode resultar em ação disciplinar, incluindo até mesmo a demissão da Ipsos.

2. Escopo

Esta Política se aplica globalmente a todas as empresas Ipsos, independentemente de onde estejam sediadas. Na Ipsos, esta Política formará o padrão mínimo ao qual todas as empresas Ipsos, empregados e fornecedores devem aderir, independentemente da aplicabilidade do GDPR a qualquer atividade ou território específico.

Qualquer pessoa que trabalhe para a Ipsos tem algum grau de responsabilidade por garantir que Dados Pessoais sejam coletados, armazenados e tratados de maneira adequada.

É responsabilidade de todos que os Dados Pessoais sejam processados e tratados de acordo com esta Política e seus princípios de proteção de dados.

A Ipsos também espera que seus fornecedores/vendedores cumpram os princípios aqui estabelecidos.

3. Aplicação de Leis Nacionais e Códigos de Conduta

Esta Política de Proteção de Dados adota princípios de privacidade aceitos internacionalmente, conforme aprimorados pelo GDPR. Ela se aplica subsidiariamente e complementa qualquer legislação nacional aplicável. As leis nacionais pertinentes prevalecerão caso haja um conflito com esta Política ou caso tenham requisitos mais rígidos do que esta Política. Quaisquer requisitos de registro, notificação ou relatório para o tratamento de dados conforme as leis nacionais devem ser observado. O conteúdo desta Política também deve ser observado na ausência de legislação nacional correspondente.

Cada empresa do Grupo Ipsos é responsável pelo cumprimento desta Política de Proteção de Dados e das obrigações legais aplicáveis. Havendo razões para crer que as obrigações legais contradizem os deveres estabelecidos nesta Política de Proteção de Dados, a empresa do Grupo deverá informar o Encarregado pela Proteção de Dados (DPO) do país e o Diretor Global de Privacidade Corporativa (CPO). Caso haja conflito entre a legislação nacional e a Política de Proteção de Dados, a Ipsos trabalhará juntamente com a sociedade aplicável para encontrar uma solução prática que cumpra os requisitos e atenda os fins desta Política, assim como da legislação aplicável.

Além desta Política, para o seu negócio de pesquisas de mercado, a Ipsos adere aos requisitos

do Código Internacional ICC/Esomar de Mercado, Opinião e Pesquisa Social e Análise de Dados, o qual pode ser encontrado aqui.

4. Princípios para o Tratamento de Dados Pessoais

- Todos os Dados Pessoais devem ser tratados de forma adequada, independentemente de como são coletados, registrados e processados - quer seja em papel, em um arquivo de computador, base de dados ou registrados em outros materiais e há princípios comumente aceitos para salvaguardar isto, conforme estabelecidos nas Diretrizes da OCDE a respeito da Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, assim como medidas de segurança aplicáveis em diversos estatutos ao redor do mundo, incluindo o GDPR.

A Ipsos considera o tratamento legítimo e correto de Dados Pessoais e a manutenção da confiança daqueles com os quais lida um componente vital de suas operações comerciais, comprometendo-se a agir de forma ética e responsável no que diz respeito a estes Dados Pessoais, bem como a sempre oferecer um alto grau de confidencialidade e segurança.

Para demonstrar estes compromissos, a Ipsos adere aos princípios relativos ao tratamento de Dados Pessoais previstos na GDPR que são, em si, uma materialização dos princípios da OCDE. A Ipsos respeita os seguintes princípios relativos a Dados Pessoais, que serão explicados de forma mais detalhada adiante, que determinam que tais dados sejam:

- Tratados de maneira justa e legítima.
- Tratados para finalidade específica e de forma adequada.
- Adequados, relevantes e não excessivos para a finalidade.
- Precisos.
- Mantidos pelo tempo necessário para a finalidade, sem excedê-lo.
- Tratados de forma alinhada aos direitos dos Titulares de Dados.
- Mantidos em segurança.
- Que não sejam transferidos a pessoas ou organizações situadas em outros países sem proteção adequada.

4.1. Legalidade, Equidade e Transparência

Os Dados Pessoais devem ser tratados e coletados de forma legal, justa e transparente em relação ao Titular de Dados. Ainda, Titulares de Dados devem ser informados sobre como seus dados estão sendo tratados. Em geral, Dados Pessoais devem ser coletados diretamente do indivíduo em questão. Quando não for o caso, o fundamento legal segundo o qual se justifica o tratamento deve estar documentado. O Encarregado pelo tratamento de Dados Pessoais deve ser consultado sobre se o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser conduzido (consultar também o guia separado sobre RIPDs que pode ser encontrado na intranet).

4.2. Finalidade Específica do Tratamento

Os Dados Pessoais devem ser coletados apenas para finalidades específicas, explícitas e legítimas e não serão tratados de maneira incompatível ou que exceda tais finalidades. Alterações subsequentes à finalidade são possíveis apenas de forma limitada e exigem fundamentação e validação. O DPO (Encarregado) competente deve ser consultado sobre se o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser conduzido (consultar também o guia separado sobre RIPDs que pode ser encontrado na intranet).

4.3. Minimização de Dados

Os Dados Pessoais devem ser adequados, relevantes e limitados àquilo que é necessário em relação à finalidade para a qual são tratados. Deve-se determinar se e em que medida o tratamento de Dados Pessoais é necessário para cumprir a finalidade para a qual o tratamento é empreendido. Onde a finalidade o permitir e onde o gasto envolvido for proporcional ao objetivo pretendido, dados anonimizados devem ser utilizados em vez de Dados Pessoais.

4.4. Exatidão

Os Dados Pessoais devem ser exatos e, onde necessário, mantidos atualizados; todas as medidas razoáveis devem ser tomadas para garantir que os Dados Pessoais que sejam imprecisos, tendo em conta a finalidade para a qual são tratados, sejam apagados ou corrigidos sem demora.

4.5. Prazo de Armazenamento

Os Dados Pessoais não devem ser mantidos de uma maneira que permita a identificação dos Titulares de Dados por mais tempo do que necessário para atingir a finalidade para a qual os Dados Pessoais são tratados. A Ipsos não manterá Dados Pessoais por mais tempo que o necessário para a finalidade ou finalidades para as quais eles foram coletados. A Ipsos tomará todas as medidas razoáveis para destruir ou apagar de seus sistemas todos os Dados Pessoais que não sejam mais necessários.

4.6. Integridade e Confidencialidade

Os Dados Pessoais devem ser tratados de forma a garantir a segurança adequada para que não sejam revelados, disseminados, acessados ou manipulados. Portanto, onde metodologicamente possível e onde os gastos não forem desproporcionais aos riscos do Titular de Dados, dados pseudonimizados devem ser utilizados para o tratamento - LEMBRETE: dados pseudonimizados continuam sendo e são Dados Pessoais!

4.7. Restrição a Transferências

Dados Pessoais não devem ser transferidos a outros países (nem mesmo para outras empresas Ipsos em tais países) que não ofereçam um nível adequado de proteção. A Ipsos introduziu várias medidas para assegurar tal nível adequado de proteção, de forma geral (consultar também o parágrafo 6 para obter mais detalhes), no entanto, diversos países podem ter requisitos adicionais e/ou diferentes aos quais se deve aderir.

4.8. Medidas e Considerações Gerais

Adicionalmente ao que concerne ao seus negócios de pesquisas de mercado, a Ipsos cumpre o Código Internacional de Mercado, Opinião e Pesquisa Social e Análise de Dados da ICC/ESOMAR e a Lista de Verificação de Proteção de Dados da Esomar.

5. Bases Legais para o Tratamento de Dados

A Ipsos coletará, tratará e utilizará Dados Pessoais apenas sob as seguintes bases legais, considerando sempre que tal base legal exista sob a legislação nacional aplicável. Uma destas bases legais também é exigida se a finalidade de coletar, processar e utilizar os Dados Pessoais for alterada em relação à finalidade original, a não ser que haja uma compatibilidade clara entre a finalidade original e a nova finalidade. Consultar também o parágrafo 4.2 e quaisquer possíveis requisitos adicionais de conformidade.

5.1. Dados do Respondente

Respondentes são os Titulares de Dados mais comuns nos negócios da Ipsos. Consequentemente, o tratamento correto de seus Dados Pessoais está no cerne do negócio da Ipsos.

5.1.1. Consentimento para o Tratamento de Dados

Dados Pessoais podem ser tratados após o consentimento do Titular de Dados. Antes de consentir, o Titular de Dados deve ser informado de acordo com o princípio de transparência conforme estabelecido no parágrafo 4.1. A declaração de consentimento deve ser obtida por escrito ou de forma eletrônica para os fins de documentação. Em algumas circunstâncias, tais como entrevistas por telefone, o consentimento pode ser dado verbalmente. Em todos os casos, a concessão do consentimento deve ser documentada.

Qualquer consentimento será válido apenas se constituir uma indicação expressa de forma livre, específica, informada e inequívoca dos desejos do Titular de Dados que, ao dar uma declaração ou por meio de uma ação afirmativa, indique a concordância com o tratamento de Dados Pessoais em relação a ele/ela. Para obter orientações a respeito do consentimento, favor consultar a intranet.

5.1.2. Tratamento de Dados para uma Relação Contratual

Além do consentimento, seus Dados Pessoais podem ser tratados quando necessário no contexto de um contrato do qual tais Titulares de Dados sejam parte, a fim de cumprir obrigações e deveres aplicáveis. Isto também se aplica quando tal tratamento é necessário para firmar ou rescindir um contrato. Isto se aplica em especial a respondentes (incluindo clientes misteriosos) ao se inscreverem para painéis da Ipsos.

Alguns países vêem a celebração de um contrato como uma forma de consentimento.

5.1.3. Tratamento de Dados para Cumprimento de Obrigação Legal

O tratamento de Dados Pessoais também é permitido caso a legislação nacional o solicite, exija ou permita. O tipo e extensão de tratamento de dados deve ser necessário para a atividade legalmente autorizada de tratamento de dados e deve cumprir as disposições legais aplicáveis.

5.1.4. Tratamento de Dados Conforme Interesse Legítimo

Os Dados Pessoais também podem ser tratados, caso seja necessário para os interesses legítimos do grupo Ipsos e onde a legislação nacional prevê esta base (p. ex. Artigo 6(1)(f) do GDPR). A base jurídica de interesse legítimo para tratamento não é reconhecida em todos os países e a legislação nacional pertinente terá precedência. Em geral, Dados Pessoais Sensíveis não podem ser processados com base em interesse legítimo! Em todo caso, os Dados Pessoais não podem ser tratados com base em um interesse legítimo se, em um caso individual, houver evidências de que os interesses do Titular de Dados mereçam proteção e que esta proteção tenha prevalência. Antes que os Dados Pessoais sejam tratados com base no interesse legítimo, é necessário determinar se há um interesse que mereça proteção e uma avaliação de interesse legítimo (na forma de um RIPD com uma ênfase especial no interesse legítimo) deve ser conduzida pela respectiva empresa do grupo Ipsos. Qualquer uma destas avaliações deve ser validada pelo DPO (Encarregado) ou pelo CPO (Diretor Global de Privacidade Corporativa).

5.1.5. Tratamento de Dados Pessoais Sensíveis

Dados Pessoais Sensíveis, ou, pelo GDPR, Categorias de Dados Especiais, podem ser processados apenas caso a lei o exija ou caso o Titular de Dados tenha concedido seu consentimento explícito. Para obter orientações a respeito do consentimento, favor consultar a intranet. Dados Pessoais Sensíveis também podem ser processados caso seja obrigatório para reivindicar, exercer ou defender ações judiciais. Dentro do Espaço Econômico Europeu, Dados Pessoais Sensíveis também podem ser tratados para pesquisa científica e histórica e para fins estatísticos (Artigo 9(2)(j)), sujeito a medidas adicionais adequadas. Antes de confiar nestas disposições, deve-se consultar o DPO ou CPO, bem como a legislação nacional aplicável.

5.1.6. Dados do Usuário e Internet

Se Dados Pessoais forem coletados, tratados e utilizados em sites ou em aplicativos, o Titular de

Dados deve ser informado a respeito disto em uma declaração de privacidade incluindo, se aplicável, informações sobre cookies ou medidas técnicas similares. A declaração de privacidade e quaisquer informações sobre cookies devem ser integradas de forma que sejam fáceis de identificar, diretamente acessíveis, fáceis de entender e continuamente disponíveis pelo e para o Titular de Dados.

Se perfis de uso ("tracking") forem criados para avaliar o uso de sites e aplicativos, os Titulares de Dados devem ser sempre informados adequadamente na declaração de privacidade. O "tracking" de Titulares de Dados online só pode ser realizado se permitido sob legislação nacional ou mediante consentimento explícito dos Titulares de Dados. Mesmo que o "tracking" utilize um pseudônimo para o Titular de Dados, o Titular de Dados deve ter a chance de optar pela desativação, na declaração de privacidade. Em relação à medição de audiência online sem registro prévio, a Ipsos também adere aos princípios promulgados por researchchoices.com.

Se sites ou aplicativos podem acessar Dados Pessoais em uma área restrita a usuários/respondentes registrados, a identificação e autenticação do Titular de Dados deve oferecer proteção suficiente durante o acesso.

Como parte do compromisso da Ipsos em aderir ao Código Esomar, as regras e requisitos estabelecidos no Guia de Pesquisa em Rede Social, Diretriz de Pesquisa Online e Diretriz de Pesquisa e Análise de Dados com Crianças, Jovens e Outros Indivíduos Vulneráveis da Esomar também se aplicam à Ipsos, como parte desta política.

5.2. Dados Pessoais Fornecidos por Clientes

A transmissão de Dados Pessoais à Ipsos por seus clientes é uma ocorrência comum. Ele geralmente acontece para nos oferecer uma amostra ou para aprimorar uma amostra existente. Em relação a quaisquer Dados Pessoais recebidos desta maneira, a Ipsos será o Operador e apenas poderá tratar estes Dados Pessoais de acordo com as instruções pactuadas com ou recebidas do cliente. Estas instruções podem incluir restrições a transferências a outras partes (incluindo outras empresas Ipsos) ou transferências a outros países, assim como requisitos específicos de segurança. Quaisquer restrições tais devem ser cumpridas. É fundamental que tais instruções sejam documentadas por escrito e compactuadas antes que quaisquer acordos contratuais aplicáveis sejam aceitos pela Ipsos, a fim de garantir que a Ipsos é capaz, de fato, de cumprir quaisquer restrições ou requisitos específicos de clientes.

Independentemente de quaisquer requisitos de clientes, quaisquer Dados Pessoais fornecidos por um cliente podem ser apenas:

a) Tratados para a finalidade para a qual foram fornecidos;
b) Mantidos pelo tempo exigido para a finalidade, sem excedê-lo;
c) Sujeitos aos mesmos requisitos de segurança aplicáveis aos Dados Pessoais da própria Ipsos.

5.3. Dados de Empregados

5.3.1. Tratamento de Dados na Relação de Emprego

Em relações de trabalho, os Dados Pessoais podem ser tratados, caso sejam necessários para iniciar, executar ou rescindir o contrato de trabalho. Ao iniciar uma relação de trabalho, os Dados Pessoais do candidato podem ser tratados. Caso o candidato seja rejeitado, seus dados devem ser deletados em atenção ao prazo de retenção, a não ser que o candidato tenha concordado em permanecer no arquivo para um processo seletivo futuro. O consentimento também é necessário para utilizar os dados para processos adicionais de candidatura antes de compartilhar a candidatura com outras empresas do grupo Ipsos.

Na relação de trabalho existente, o tratamento de dados deve estar sempre relacionado à finalidade do contrato de trabalho, se nenhuma das circunstâncias a seguir para tratamento autorizado de dados for aplicável.

Caso seja necessário coletar informações sobre um candidato a partir de um terceiro, durante o processo de candidatura, os requisitos das leis nacionais correspondentes devem ser observados. Caso haja dúvidas, o consentimento dos Titulares de Dados deve ser obtido.

Deve haver base legal para processar os Dados Pessoais relativos à relação de emprego, mas que não eram originalmente parte da execução do contrato de trabalho. Isto pode incluir obrigações legais, regulamentos coletivos com representantes dos empregados, consentimento do empregado ou o interesse legítimo da empresa.

5.3.2. Tratamento de Dados Conforme Obrigação Legal

Favor consultar acima o parágrafo 5.1.3 para obter os requisitos adicionais.

5.3.3. Acordos Coletivos de Tratamento de Dados

Caso uma atividade de tratamento de dados exceda as finalidades de cumprimento de contrato, ela pode ser admissível se autorizada através de um acordo coletivo entre o empregador e os representantes dos funcionários, dentro do escopo permitido sob a lei trabalhista aplicável. Os acordos devem abranger a finalidade específica da atividade pretendida de tratamento adicional de dados e devem ser elaborados dentro dos parâmetros da legislação nacional de proteção de dados e laboral.

5.3.4. Consentimento para o Tratamento de Dados

Os dados dos empregados podem ser tratados mediante seu consentimento. Declarações de consentimento devem ser apresentadas voluntariamente. Dentro da União Europeia/do Espaço Econômico Europeu, o consentimento geralmente não constitui uma base legal válida para o tratamento em um contexto de trabalho, uma vez que há uma presunção legal de que tal consentimento não foi apresentado voluntariamente e qualquer tratamento terá de depender de uma das outras bases legais disponíveis. O consentimento involuntário é nulo. Na medida em que o consentimento é uma base válida para o tratamento, veja o item 5.1.1 acima para requisitos adicionais. Uma complicação adicional é que o consentimento normalmente pode ser retirado, impedindo, assim, qualquer tratamento adicional.

5.3.5. Tratamento de Dados Conforme Interesse Legítimo

Os Dados Pessoais também podem ser tratados para atender um interesse legítimo do grupo Ipsos, quando a lei aplicável permite o processamento de Dados Pessoais com base em um interesse legítimo. Dentro do contexto de trabalho, interesses legítimos são geralmente de natureza legal ou financeira.

Favor consultar acima o parágrafo 5.1.4 para mais requisitos e limitações do interesse legítimo.

Medidas de controle ou supervisão que exijam o tratamento de dados de empregados podem ser tomadas apenas se houver uma obrigação legal de fazê-lo ou se houver um motivo legítimo. Ainda que haja um motivo legítimo, a proporcionalidade das medidas de controle também deve ser examinada antes de sua aplicação. O interesse justificado da empresa em executar a medida de controle (p. ex. cumprimento de regras internas da empresa ou interesses de segurança) deve ser considerado em relação a qualquer interesse do empregado que mereça proteção e que possa excetuar a aplicação da medida, que será executada apenas se considerada apropriada. Os interesses legítimos da empresa e quaisquer interesses do empregado que mereçam proteção devem ser identificados e documentados antes que quaisquer medidas sejam adotadas por meio de uma avaliação de interesse legítimo. Além disto, quaisquer requisitos adicionais nos termos das leis nacionais (p. ex. direitos de co-determinação para os representantes dos empregados e direitos de informação dos Titulares de Dados) devem ser levados em consideração.

5.3.6. Tratamento de Dados Pessoais Sensíveis

Dados Pessoais Sensíveis (Categorias Especiais de Dados) podem ser processados apenas caso a lei o exija ou caso os Titulares de Dados tenham concedido seu consentimento explícito. Estes dados também podem ser tratados caso seja obrigatório para reivindicar, exercer ou defender ações judiciais.

5.3.7. Decisões com Tratamento Automatizado de Dados Pessoais

Se Dados Pessoais forem tratados de forma automatizada como parte de uma relação de trabalho e detalhes pessoais específicos forem avaliados para a tomada de decisão (p. ex. parte do processo seletivo do quadro de funcionários ou a avaliação de pontuações), este tratamento automatizado não pode ser o único fundamento para decisões que teriam consequências negativas ou criariam problemas significativos para as pessoas afetadas. A fim de evitar decisões equivocadas, o tratamento automatizado deve garantir que uma pessoa física avalie o conteúdo da situação e que esta avaliação seja o fundamento para sua decisão. Os Titulares de Dados também devem ser informados a respeito dos fatos e resultados das decisões individuais tomadas unicamente com base em tratamento automatizado e da possibilidade de responder.

5.3.8. Telecomunicações e Internet

Equipamentos de telefone, endereços de e-mail, intranet e Internet, juntamente com redes sociais internas são fornecidos pela Ipsos primordialmente para tarefas relacionadas ao trabalho. Eles são uma ferramenta e um recurso da empresa. Eles podem ser utilizados dentro dos regulamentos legais aplicáveis e políticas internas da empresa, especialmente a Política de Segurança da Informação & Uso Aceitável. Em caso de utilização autorizada para fins privados, deverá ser observada a lei do sigilo das telecomunicações nas respectivas legislações nacionais de telecomunicações, quando aplicável.

A Ipsos está utilizando tecnologia de filtragem de web para assegurar a conformidade com sua Política de Uso Aceitável, medição e análise de tráfico de internet, outras obrigações legais de conformidade e para se defender de ataques à infraestrutura de TI ou usuários individuais. Medidas de proteção podem ser implementadas para as conexões à rede Ipsos que bloqueiam conteúdo tecnicamente nocivo e para analisar os padrões de ataque. Por motivos de segurança, o uso de equipamento de telefone, endereços de e-mail, intranet/Internet e redes sociais internas pode ser bloqueado de forma permanente ou temporária para endereços/localizações individuais ou tipos de conexão. Avaliações destes dados por parte de uma pessoa específica podem ser feitas apenas em um caso concreto e justificado de suspeitas de violação a leis ou políticas do grupo Ipsos e devem ser autorizadas por qualquer uma das pessoas que podem autorizar uma "retenção legal" (consultar também a Política de Gerenciamento de Informação de TI). As leis nacionais aplicáveis devem ser observadas da mesma maneira que os regulamentos do grupo.

5.4. Contatos de Marketing

Em geral, contatos de marketing não são diferentes de respondentes no que diz respeito às proteções de privacidade dedicadas a eles. Suas informações de contato constituem Dados Pessoais, ainda que sejam relacionados aos negócios. Apenas se as informações de contato forem realmente genéricas tais como “contato@acme.com”, elas não estarão sujeitas a esta Política.

Comunicações de marketing frequentemente estão sujeitas a requisitos legais específicos, especialmente se forem enviadas eletronicamente ou feitas por telefone.

Deve-se presumir que os contatos de marketing não tenham solicitado os materiais de marketing. Ou seja, os destinatários não pediram para receber comunicações de marketing da Ipsos. Para agir de forma legal, as condições concernentes à base legal, especialmente, requisitos de consentimento estabelecidos no parágrafo 5.1.1 também se aplicam aqui.

Excepcionalmente, uma 'soft opt-in' (envio de e-mails para contatos já existentes, porém sempre oferecendo a opção de desabilitar) pode ser aplicada, caso as condições abaixo sejam cumpridas:

- quando as informações do Titular de Dados foram obtidas no decurso de uma venda ou negociações para a venda de serviços da Ipsos;
- quando as mensagens sejam apenas serviços similares a marketing; e onde é dada à pessoa uma oportunidade simples de recusar o marketing quando suas informações são coletadas, e se eles não optarem pelo não recebimento a esta altura, que tenham uma maneira simples de fazê-lo em todas as mensagens futuras.

6. Transferência de Dados Pessoais

A Transferência de Dados Pessoais a destinatários fora ou dentro do Grupo Ipsos está sujeita aos requisitos de autorizaçãopara o tratamento de Dados Pessoais no item 4.7, Restrição a

Transferências. O destinatário de dados (quer este seja outra empresa Ipsos ou qualquer subcontratante) deve ser obrigado a utilizar os dados apenas para as finalidades definidas. Para transferências externas, os requisitos deste parágrafo e aqueles do parágrafo 7, Tratamento de Dados Subcontratado ou Realizado Por Terceiros aplicam-se de maneira cumulativa.

Se Dados Pessoais forem enviados a um destinatário fora do Grupo Ipsos baseado em outro país, este destinatário deve concordar expressamente em manter o nível de proteção de dados equivalente a esta Política de Proteção de Dados ou conforme exigido pela legislação aplicável. Por exemplo, o GDPR estipula diversos requisitos que devem ser cumpridos, antes que qualquer transferência possa ocorrer. Isto não se aplica se a transferência for fundamentada em um dever legal. Um dever legal deste tipo pode se basear nas leis do país de domicílio da empresa do grupo Ipsos que estiver enviando os dados. Alternativamente, as leis do país de domicílio da empresa do grupo Ipsos pode reconhecer a finalidade da transferência de dados com base nos deveres legais de um país terceiro.

Quando os Dados Pessoais forem enviados por um terceiro (como um fornecedor de amostras) a uma empresa do grupo Ipsos, deve-se assegurar que os Dados Pessoais possam ser utilizados para a finalidade pretendida.

Se os Dados Pessoais forem transferidos de uma empresa do Grupo Ipsos com a sua sede social em um país para uma empresa do grupo Ipsos com a sua sede social em outro país, a empresa que estiver importando os dados tem a obrigação de cooperar com os inquéritos feitos pela autoridade supervisora pertinente no país em que a parte que exporta os dados tem a sua sede social e a cumprir quaisquer observações feitas pela autoridade supervisora no que diz respeito ao tratamento dos dados enviados.

Se um Titular de Dados alegar que esta Política de Proteção de Dados foi violada por uma empresa do grupo Ipsos localizada em outro país que esteja importando os dados, a empresa do grupo Ipsos que estiver exportando os Dados Pessoais se responsabilizará por dar assistência ao Titular de Dados em questão, ao estabelecer os fatos nesta questão e também ao reivindicar seus direitos de acordo com sua Política de Proteção de Dados em relação à empresa do grupo Ipsos que esteja importando os dados. Além disto, os Titulares de Dados também têm o direito de reivindicar seus direitos em relação à empresa do grupo Ipsos que estiver exportando os dados. No caso de reclamações de uma violação, a empresa exportadora deve documentar para os Titulares de Dados que a empresa que estiver importando os Dados Pessoais não violou esta Política de Proteção de Dados.

Cada empresa do Grupo Ipsos que estiver enviando Dados Pessoais à empresa do Grupo Ipsos localizada em outro país deverá permanecer responsável por quaisquer violações desta Política de Proteção de Dados cometidas pela empresa do Grupo Ipsos que recebeu os Dados Pessoais, como se a violação tivesse sido cometida pela empresa do Grupo Ipsos que estiver enviando os Dados Pessoais.

Qualquer transferência de Dados Pessoais dentro do Grupo Ipsos deve ser feita somente após um registro relevante no JobBook para o projeto sob o qual a transferência ocorre. Tal registro criará um contrato ao abrigo do Intergroup Master Service Agreement da Ipsos e automaticamente tornará as respectivas Cláusulas Modelo da UE aplicáveis a tal transferência.

7. Tratamento de Dados Realizado por Subcontratados ou Por Terceiros

Em muitos casos, a Ipsos utiliza fornecedores externos para processar Dados Pessoais. Nestes casos, um acordo de tratamento de dados em nome da Ipsos deve ser celebrado com tal fornecedor. Isto pode ser feito tanto através da inclusão de disposições apropriadas no contrato que rege a relação geral com o fornecedor quanto em um documento separado e específico. Em relação ao tratamento em nome da Ipsos, o fornecedor apenas pode processar os Dados Pessoais de acordo com as instruções da Ipsos. Ao instruir um fornecedor, os seguintes requisitos devem ser cumpridos:

- Onde os Dados Pessoais em questão se enquadrarem no parágrafo 5.2 (dados de clientes), quaisquer requisitos relevantes dos clientes devem ser repassados ao fornecedor.
- O fornecedor deve ser escolhido com base em sua capacidade de atender às medidas técnicas e organizacionais de proteção exigidas e de forma alinhada ao processo de aprovação de fornecedores da Ipsos.
- O fornecedor não deve subcontratar o tratamento sem o consentimento prévio por escrito

da Ipsos.

- As instruções devem ser apresentadas por escrito por meio de um contrato apropriado. As instruções a respeito do tratamento de dados e as responsabilidades da Ipsos e do fornecedor devem ser documentadas.
- Antes que o tratamento de dados tenha início, a Ipsos deve ter certeza de que o fornecedor cumprirá com suas obrigações. Um fornecedor pode documentar seu cumprimento dos requisitos de segurança de dados, em particular, apresentando certificação adequada. A depender do risco do tratamento de dados, as revisões devem ser repetidas regularmente durante o período de vigência do contrato. A Ipsos deve reter o direito de auditar o cumprimento do fornecedor.
- No caso de um contrato de tratamento de dados transnacional, os requisitos nacionais relevantes para a divulgação de Dados Pessoais no exterior devem ser cumpridos. Em especial, os Dados Pessoais do Espaço Econômico Europeu podem ser tratados em um país terceiro apenas se o fornecedor puder provar que possui um padrão de proteção de dados equivalente ao GDPR e esta Política de Proteção de Dados. Podem ser ferramentas adequadas:
    - um contrato baseado em cláusulas contratuais padrão da UE para tratamento de dados contratuais em países terceiros com o fornecedor. Contratos similares serão exigidos para qualquer subcontratante do fornecedor.
    - A participação do fornecedor em um sistema de certificação acreditado pela UE para o oferecimento de um nível suficiente de proteção de dados.

8. Direitos de Titulares dos Dados

Todos os Titulares de Dados têm os direitos aqui previstos. Sua solicitação deve ser tratada imediatamente pela empresa do grupo Ipsos responsável, e não deve resultar em qualquer desvantagem para o Titular de Dados. Quando os Dados Pessoais relevantes estiverem sendo tratados pela Ipsos, de acordo com o parágrafo 5.2 Dados Pessoais Fornecidos por Clientes, o contrato aplicável com o cliente deve ser consultado no que se refere a qualquer processo a ser seguido e o cliente deve ser informado a respeito de tal solicitação, imediatamente.

- **Direito de acesso:**
    - Os Titulares de Dados podem solicitar informações a respeito de quais Dados Pessoais relativos a eles foram armazenados, como os dados foram coletados e com qual finalidade.
    - Se Dados Pessoais forem transferidos a terceiros, informações a respeito da identidade do destinatário ou a respeito das categorias de destinatários, incluindo outras empresas Ipsos, devem ser fornecidas.
- **Direito à retificação:** Caso os Dados Pessoais estejam incorretos ou incompletos, o Titular de Dados pode exigir que eles sejam corrigidos ou aditados.
- **Direito de retirar o consentimento:** Onde os Dados Pessoais são tratados com base no Consentimento (consultar também as orientações separadas sobre Consentimento), os Titulares de Dados podem se opor ao tratamento, a qualquer momento. Estes Dados Pessoais devem ser bloqueados para o tratamento ao qual se fez oposição.
- **Direito a eliminação.** O Titular de Dados pode solicitar que seus dados sejam eliminados se o tratamento de tais dados não tiver base legal ou caso a base legal não seja mais aplicável. O mesmo vale se a finalidade para o tratamento de dados tiver prescrito ou deixado de ser aplicável por outros motivos. Deverão ser observados os períodos de retenção em relação a interesses conflitantes que mereçam proteção.
- **Direito de objeção:** Titulares de Dados têm, geralmente, o direito de fazer objeção ao tratamento de seus dados e isto deve ser levado em consideração se a proteção de seus interesses prevalecer sobre os interesses do controlador de dados em razão de situação pessoal particular. Isto não se aplica no caso de obrigação legal exigir o tratamento de tais Dados Pessoais.
- **Direito à portabilidade de dados.** O Titular de Dados tem o direito de solicitar que os Dados Pessoais por ele/ela fornecidos sejam disponibilizados em um formato fácil de ler, como um documento de Word ou Excel.

9. Confidencialidade no Tratamento

Dados Pessoais estão sujeitos à confidencialidade da informação. Qualquer coleta, tratamento ou uso não autorizado de tais dados por parte de empregados é proibido. Qualquer tratamento de dados realizado por um empregado sem que tenha recebido a atribuição de realizar tal tratamento como parte de suas funções legítimas não é autorizado. Aplica-se o princípio da

"necessidade de conhecer". Os Empregados podem ter acesso aos Dados Pessoais no limite apropriado para o tipo e escopo da tarefa que desempenharão. Isto exige papeis e responsabilidades cuidadosamente delimitados e distribuídos, incluindo limitações. Adicionalmente, os requisitos da Política de Gerenciamento de Informações se aplicam.

Empregados são proibidos de utilizar Dados Pessoais para suas próprias finalidades pessoais ou comerciais, de divulgá-los a pessoas não autorizadas, ou de disponibilizá-los de qualquer outra forma. Os supervisores devem informar os empregados no início da relação de trabalho a respeito da obrigação de manter o sigilo de dados. Esta obrigação permanecerá em vigor mesmo depois de encerrada a relação de trabalho. Os contratos de trabalho dos empregados da Ipsos devem conter obrigações apropriadas de confidencialidade.

10. Privacidade desde o princípio e por princípio

A Ipsos utilizará uma abordagem de Privacidade desde o princípio e por princípio em todos os seus trabalhos, mas especialmente ao:

- construir novos sistemas de TI para armazenar ou acessar dados pessoais;
- desenvolver novos aplicativos ou abordagens de pesquisa;
- embarcar em uma iniciativa de compartilhamento de dados; ou
- utilizar dados para novas finalidades.

A privacidade desde o princípioé uma abordagem que promove a privacidade e o cumprimento da proteção de dados em projetos, desde seu início. Trata-se de uma consideração fundamental nas etapas iniciais de qualquer projeto e, posteriormente, no decorrer de sua vida útil.

Utilizar uma abordagem de privacidade desde o princípioé uma ferramenta essencial para minimizar riscos à privacidade e para criar confiança e determinação na concepção de projetos, processos, produtos ou sistemas tendo em mente a privacidade, desde o princípio.

No que diz respeito aos exemplos fornecidos acima, a ferramenta exigida para o cumprimento é a execução de um Relatório de Impacto à Proteção de Dados.

11. Segurança no Tratamento

Os Dados Pessoais devem ser protegidos de acesso ou divulgação não autorizados (quer sejam causados internamente ou externamente), tratamento ilegal, assim como perda, modificação ou destruição acidental. Isto se aplica independentemente de os dados serem tratados de forma eletrônica ou em papel. Além de proteger Dados Pessoais existentes alinhados com as políticas relevantes da Ipsos (favor consultar o Capítulo 7 do Livro de Políticas e Procedimentos da Ipsos, que se aplica a este respeito), antes da introdução de novos métodos de tratamento de dados, alguns novos sistemas de TI ou abordagens de pesquisa, medidas técnicas e organizacionais para proteger Dados Pessoais devem ser definidos e implementados. Estas medidas devem se basear no estado da arte, no risco de tratamento e na necessidade de proteger os dados. Estas medidas técnicas e organizacionais devem ser acordadas em colaboração com o Responsável pela Segurança da Informação e o DPO. As medidas técnicas e organizacionais para proteger os Dados Pessoais fazem parte do gerenciamento de Segurança de Informações Corporativas e devem ser continuamente adaptadas ao desenvolvimento e aos avanços técnicos, assim como às mudanças organizacionais.

No mínimo, a Ipsos processará todos os Dados Pessoais que detém de acordo com a sua Política de Segurança e tomará as medidas de segurança apropriadas contra o tratamento ilegal ou não autorizado de Dados Pessoais e contra a perda acidental de, ou o dano acidental a, Dados Pessoais.

12. Auditoria de Proteção de Dados

O cumprimento desta Política de Proteção de Dados e das leis aplicáveis de proteção de dados é verificado regularmente através de auditorias de proteção de dados e outros controles. A execução destes controles é de responsabilidade do CPO, do DPO, da Auditoria Interna e/ou de auditores

contratados externamente. Diversos clientes da Ipsos também possuem direitos de auditoria de acordo com seus contratos com a Ipsos. Os resultados das auditorias de proteção de dados devem ser reportados ao CPO e ao Líder de Compliance. Mediante solicitação, os resultados das auditorias de proteção de dados serão disponibilizados para as autoridades responsáveis pela proteção de dados.

13. Incidentes de Proteção de Dados

Todos os empregados devem informar seu DPO ou CPO imediatamente sobre casos de violações desta Política de Proteção de Dados ou de outros regulamentos de proteção de Dados Pessoais, de acordo com o Procedimento de Gerenciamento de Violação a Dados Pessoais, o qual também pode ser encontrado na Seção 8 do Livro de Políticas e Procedimentos da Ipsos. Qualquer omissão em lidar com falhas graves segundo esta Política também pode ser reportada no sistema de Denúncias da Ipsos.

Em caso de:

- transferência indevida de Dados Pessoais a terceiros;
- transferência indevida de Dados Pessoais, internacionalmente;
- acesso indevido, inclusive por terceiros, a Dados Pessoais, ou
- perda de Dados Pessoais (inclusive tornados públicos devido a falhas internas).

uma notificação de violação à proteção de dados deve ser realizada imediatamente para garantir que: a) qualquer obrigação de prestação de contas ao abrigo da legislação nacional possa ser cumprida; b) qualquer cliente afetado possa ser informado; e c) qualquer comunicação a partes interessadas possa ser gerenciada. Qualquer violação à Proteção de Dados também constituirá um incidente de segurança de informações, de acordo com a política de Gerenciamento de Incidentes de TI.

14. Responsabilidades e Sanções

14.1. Gestão

Os órgãos executivos das respectivas empresas do Grupo Ipsos são responsáveis pelo tratamento de dados em sua área de responsabilidade. Portanto, eles são obrigados a garantir que os requisitos legais e aqueles contidos nesta Política de Proteção de Dados para a proteção de dados sejam cumpridos (p. ex. obrigações nacionais de prestação de contas).

A administração é responsável por assegurar que medidas organizacionais, de RH e de ordem técnica, estejam em vigor para que qualquer tratamento de dados seja realizado de acordo com estes requisitos de proteção de dados.

O cumprimento destes requisitos também é responsabilidade dos empregados competentes.
Caso agências oficiais conduzam auditorias de proteção de dados, o CPO deve ser informado imediatamente. A gestão nacional competente da Ipsos deve informar o CPO quanto ao nome do DPO.
O tratamento indevido de Dados Pessoais, ou outras violações às leis de proteção aos dados, podem ser judicializados em muitos países, resultando em pedidos de indenização. Além disto, violações pelas quais empregados individuais sejam responsáveis podem levar a sanções nos termos da legislação trabalhista.

14.2. Responsáveis pela Proteção de Dados

Cada país da Ipsos será obrigado a indicar um ou mais Encarregado da Proteção de Dados ("**DPO**"). Os DPO's são as pessoas de contato interno e externo no país para proteção de dados. Eles podem realizar verificações e devem instruir os empregados sobre esta Política de Proteção de Dados e a legislação aplicável. A gestão competente deve auxiliar os DPOs em seus esforços. As principais atividades do DPO são:

- *Informar e aconselhar a organização e seus empregados a respeito de suas obrigações em cumprir com as leis aplicáveis de proteção de dados e com esta Política de Proteção de Dados.* Esta atividade será respaldada e regida pelo Grupo e por meio da rede de DPOs sob a liderança do CPO e de treinamentos.
- *Monitorar o cumprimento das leis de proteção de dados, incluindo o gerenciamento de atividades internas de proteção de dados, aconselhamento (não condução) a respeito de*

relatórios de impacto à proteção de dados; treinar a equipe e conduzir auditorias internas. Isto será respaldado e regido pelo Grupo. Auditorias, além de inspeções locais, devem ser coordenadas com a função de auditoria interna do Grupo.
- *Ser o primeiro ponto de contato para autoridades nacionais e para indivíduos cujos dados sejam tratados (empregados, clientes, etc.).*

Em cada país da Ipsos, o DPO deverá:

- Reportar ao mais alto nível de gestão da organização nacional da Ipsos - ou seja, ao nível ou membro do conselho de gestão local.
- Operar independentemente de ordens profissionais, não sendo dispensado ou penalizado por executar sua tarefa.
- Deter acesso a recursos adequados que permitam ao DPO cumprir suas obrigações de acordo com as leis aplicáveis de proteção de dados e esta Política de Proteção de Dados.

Os Encarregados de Proteção de Dados deverão informar prontamente o CPO a respeito de quaisquer riscos à proteção de dados.

14.3. Diretor Global de Privacidade Corporativa

O Diretor Global de Privacidade Corporativa ("**CPO**"), por ser internamente independente de ordens profissionais, trabalha para o cumprimento dos reguladores de proteção de dados nacionais e internacionais. Ele/ela é responsável por esta Política de Proteção de Dados e supervisiona seu cumprimento.

Qualquer Titular de Dados pode entrar em contato com o CPO ou o DPO competente, a qualquer momento, para demonstrar preocupações, fazer perguntas, solicitar informações ou prestar queixas em relação a questões de proteção de dados ou segurança de dados. Caso o seja solicitado, preocupações e queixas serão tratadas de maneira confidencial.

Caso o DPO competente não possa sanar uma queixa ou resolver uma violação à Política de Proteção de Dados, o CPO deve ser consultado, imediatamente. As decisões do CPO para resolver violações à proteção de dados devem ser mantidas pela gerência da empresa em questão. Inquéritos por parte de autoridades supervisoras devem ser sempre reportados ao CPO.

15. Exceção

Em casos excepcionais, pode ser possível obter uma exceção a esta Política, antes de qualquer tratamento pretendido de Dados Pessoais afetados. Qualquer exceção só poderá ser concedida após uma avaliação abrangente do impacto da proteção de dados, para estabelecer e avaliar os riscos para qualquer Titular de Dados afetado, os riscos legais e o impacto de reputação, bem como estará sujeita à aprovação dos Serviços de Suporte ao Presidente da Ipsos.

16. Glossário

Controlador de Dados/Controlador/Controlador Conjunto

Esta é a pessoa ou organização que determina as finalidades para as quais, e a forma com que, quaisquer Dados Pessoais são tratados. É responsável por estabelecer práticas e políticas alinhadas aos requisitos legais aplicáveis.

Na maioria dos casos em que a Ipsos recebe listagens do cliente, haverá o controle compartilhado dos dados coletados. Isto se aplica aos dados por nós coletados, ainda que tenhamos assegurado aos respondentes a confidencialidade de seus dados. A responsabilidades e obrigações do controle compartilhado deverá ser documentada e esclarecida em um documento escrito.

Algumas jurisdições utilizam outras expressões para o mesmo conceito, como **Pessoa Responsável, Organização, Operador**[2] etc.

Usuários de Dados

Estes são os nossos empregados cujo trabalho envolve o tratamento de Dados Pessoais. Usuários de dados devem proteger os dados e Dados Pessoais com os quais lidam, de acordo com esta

[2] Singapore

Política e quaisquer procedimentos aplicáveis de segurança de dados, o tempo todo.

Operador de Dados ou Operador

Trata-se da pessoa ou organização, que não é um Usuário de Dados, e que processa Dados Pessoais em nome do, e com base nas instruções do, Controlador. Empregados de controladores de dados são excluídos desta definição, mas ela poderia incluir fornecedores que lidam com Dados Pessoais. Variavelmente, a Ipsos será um Controlador (p. ex. no que diz respeito a nossos membros do painel ou recrutas de amostra *ad hoc* para uma pesquisa Ipsos) ou um Operador (p. ex. no que diz respeito a uma amostra fornecida por clientes). Algumas jurisdições utilizam outras expressões para o mesmo conceito, como **Terceiro, Intermediário, Processador**[3] etc.

Titulares de Dados

Para efeitos desta Política, são todas as pessoas vivas sobre as quais a Ipsos retém Dados Pessoais. Um Titular de Dados não precisa ser nativo ou residente de um país. Todos os Titulares de Dados têm direitos legais em relação às suas informações pessoais.

Dados Pessoais

A definição de Dados Pessoais do GDPR (GDPR Artigo 4 (1)) deixa mais claro o que são Dados Pessoais e mostra que isto deve ser interpretado de maneira ampla:

"...quaisquer informações relativas a uma pessoa física identificada ou identificável ('titular de dados'); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, especialmente por referência a um identificador tal como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos à identidade física, fisiológica, genética, mental, econômica, cultural ou social de tal pessoa física".

Uma pessoa física é uma pessoa viva e o próprio GDPR não se aplica a indivíduos falecidos. No entanto, os Estados-Membros individuais podem estabelecer regras relativas ao tratamento de Dados Pessoais, mesmo em relação a pessoas falecidas.

Informações a respeito de uma empresa não constituirão Dados Pessoais.

Deve-se reconhecer que nem sempre é possível determinar com absoluta certeza, se um item ou informação individual é considerada um Dado Pessoaal. Será necessário examinar as informações gerais mantidas sobre a pessoa em questão ou os meios razoavelmente prováveis de serem usados para identificar uma pessoa.

Com os meios tecnológicos em constante evolução, mais dados se tornarão Dados Pessoais.

Tratamento

Tratamento é qualquer atividade que envolva o uso de dados. Inclui a obtenção, registro ou retenção de dados, ou a execução de qualquer operação ou conjunto de operações nos dados incluindo sua organização, modificação, recuperação, utilização, divulgação, seu apagamento ou destruição. O tratamento também inclui a transferência de Dados Pessoais.

Dados Pessoais Sensíveis (Categorias Especiais de Dados Pessoais)

"Categorias especiais de Dados Pessoais" é a nova expressão utilizada no GDPR e era anteriormente chamada de "dados sensíveis".[4] É definida agora no GDPR Artigo 9 como dados relativos à:

origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, dados genéticos [ver abaixo], dados biométricos [ver abaixo] para a finalidade de identificar de forma única uma pessoa física, dados relativos à saúde [ver abaixo] ou dados relativos à vida sexual ou orientação sexual de uma pessoa física

Nota: no Brasil é utilizada a expressão "dados pessoais sensíveis".

Para algumas destas expressões, definições mais detalhadas foram fornecidas no GDPR:

'dados genéticos' significa Dados Pessoais relativos às características genéticas herdadas ou adquiridas de uma pessoa física, as quais fornecem informações únicas a respeito da fisiologia

[3] South Africa

ou saúde de tal pessoa física e que resultam, especialmente, de uma análise de uma amostra biológica da pessoa física em questão;

'dados biométricos' significa Dados Pessoais resultantes de tratamento técnico específico em relação às características físicas, fisiológicas ou comportamentais de uma pessoa física, que permitam ou confirmem a identificação única de uma pessoa física, tais como imagens faciais ou dados dactiloscópicos;

'dados relativos à saúde' significa Dados Pessoais relativos à saúde física ou mental de uma pessoa física, incluindo a prestação de serviços de saúde, que revelam informações a respeito de seu estado de saúde;

Dados Anônimos

Definidos como informações que não se relacionam a uma pessoa física identificada ou identificável, ou com Dados Pessoais tornados anônimos de forma que o Titular de Dados não é mais identificável (GDPR Ponto 26). Deve ser diferenciado de dados que, juntamente com o uso de informações adicionais (p. ex. uma chave), poderiam ser utilizados para identificar uma pessoa física, então os dados foram meramente pseudonimizados.

Dados pseudonimizados ainda se enquadram na definição de Dados Pessoais, e os princípios/requisitos integrais do GDPR serão aplicáveis a eles.

Pseudonimização

Pseudonimização significa o tratamento de Dados Pessoais de tal maneira que os Dados Pessoais não possam mais ser atribuídos a um Titular de Dados específico sem o uso de informações adicionais, desde que tais informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais para garantir que os Dados Pessoais não sejam atribuídos a uma pessoa física identificada ou identificável. (GDPR Artigo 4(5))

Dados pseudonimizados referem-se a dados a partir dos quais os identificadores em um conjunto de informações são substituídos por identificadores artificiais, ou pseudônimos, mantidos separadamente e sujeitos a salvaguardas técnicas. Dados pseudonimizados permanecem Dados Pessoais e, portanto, todos os outros requisitos de proteção de dados continuam a se aplicar a eles!!

PII ou Informação Pessoalmente Identificável

Este termo deriva da legislação de privacidade dos Estados Unidos. Embora, de um ponto de vista prático aplicável ao dia a dia de trabalho da Ipsos, as expressões Dados Pessoais e PII possam ser tratadas como sinônimos, o uso da expressão PII no contexto do GDPR deve ser evitado, uma vez queutilizá-la impacta negativamente a nossa obrigação de demonstrar conformidade. Os reguladores são muito atentos à coerência e exatidão no uso de expressões.

PHI ou Informação Confidencial sobre a Saúde

Este termo também deriva da legislação de privacidade dos Estados Unidos, em especial, da HIPPA (Lei de Portabilidade e Responsabilidade dos Planos de Saúde). Embora, de um ponto de vista prático aplicável ao dia a dia de trabalho da Ipsos, as expressões Dados Sensíveis ou Categorias Especiais de Dados Pessoais e PII devam ser tratadas como sinônimos, o uso da expressão PII no contexto do GDPR deve ser evitado.

A principal questão a ser levada em consideração aqui é a de que certos Dados Pessoais que se enquadrariam na definição legal de PHI seriam considerados Dados Pessoais no GDPR, e não Categorias Especiais De Dados ou Dados Pessoais Sensíveis. Por exemplo, a HIPPA consideraria todas as informações em um conjunto de dados que contivesse o nome e a orientação sexual como PHI, enquanto o GDPR apenas consideraria a oriental sexual como sendo Dado Pessoal Sensível ou parte das Categorias Especiais de Dados Pessoais.

PSI ou Informação Pessoal Sensível

Hoje em dia, esta expressão está ultrapassada, tendo sido derivada da legislação anterior. Ela é amplamente sinônima a "Categorias Especiais de Dados Pessoais", conforme definido no Artigo 9 do GDPR, e esta expressão deve ser utilizada. Os reguladores esperam que a Ipsos

use a terminologia correta para demonstrar nossa conformidade como parte de nossa obrigação de prestação de contas.

Nota: No Brasil, a legislação determina o uso do termo Dados Pessoais Sensíveis, sendo necessário utilizar este termo em lugar do sugerido acima.

Controle de Documento (GDPR Art. 25)

Versão	Data	Sumário das Alterações	Autores	Aprovado por
1.0	12/04/2018	Versão aprovada para publicação	Rupert van Hullen	**Laurence Stoclet**

Revisão do documento	
Data da Revisão	12/04/2018
Versão Revisada	1.0
Alterações propostas (lista nº do capítulo e breve descrição	N/A
Comitê de Revisão	CPO, GC, CIO, MarCom
Autoridade/Comitê de Aprovação	Vice-CEO e CFO
Data Limite da Próxima	12/04/2019
Observação: Os registros nesta tabela não gerarão uma alteração no número da versão.	