



**Ipsos - Política de  
Privacidade e Proteção de  
Dados Pessoais**  
(em vigor a partir de 25 de maio de  
2018)

---

# Ipsos – Política de Privacidade e Proteção de Dados Pessoais

## Índice

1. Introdução.....	4
2. Âmbito.....	4
3. Aplicação de Leis Nacionais e de Códigos de Conduta .....	4
4. Princípios relativos ao Tratamento de Dados Pessoais.....	5
4.1. Licitude, Lealdade e Transparência.....	5
4.2. Limitação das Finalidades .....	5
4.3. Minimização dos Dados .....	5
4.4. Exatidão .....	6
4.5. Limitação da Conservação .....	6
4.6. Integridade e Confidencialidade .....	6
4.7. Restrições quanto às Transferências .....	6
4.8. Medidas e Considerações Gerais.....	6
5. Fundamentos Jurídicos para o Tratamento de Dados.....	6
5.1. Os Dados dos Entrevistados .....	7
5.1.1. Consentimento para o Tratamento de Dados .....	7
5.1.2. O Tratamento de Dados no quadro das Relações Contratuais .....	7
5.1.3. O Tratamento de Dados de acordo com uma Autorização Legal .....	7
5.1.4. O Tratamento de Dados de acordo com o Interesse Legítimo .....	7
5.1.5. O Tratamento de Categorias Especiais de Dados Pessoais .....	7
5.1.6. Os Dados dos Utilizadores e a Internet.....	8
5.2. Os Dados Pessoais Disponibilizados por Clientes .....	8
5.3. Os Dados Pessoais de Empregados .....	8
5.3.1. O Tratamento de Dados no quadro das Relações de Trabalho .....	8
5.3.2. O Tratamento de Dados de acordo com uma Autorização Legal .....	9
5.3.3. Os Acordos Coletivos sobre Tratamento de Dados .....	9
5.3.4. Consentimento para o Tratamento de Dados .....	9
5.3.5. O Tratamento de Dados de acordo com o Interesse Legítimo .....	9
5.3.6. O Tratamento de Categorias Especiais de Dados Pessoais .....	10
5.3.7. Decisões Automatizadas .....	10
5.3.8. Telecomunicações e a Internet .....	10
5.4. Contactos Comerciais .....	10
6. A Transmissão de Dados Pessoais .....	11
7. O Tratamento de Dados em Subcontratação/Por Terceiros.....	11
8. Os Direitos do Titular dos Dados .....	12
9. A Confidencialidade no Tratamento dos Dados.....	13
10. A Privacidade desde a Conceção e Por Defeito .....	13
11. A Segurança do Tratamento .....	13
12. Auditorias sobre Proteção dos Dados.....	14
13. Incidentes relativos à Proteção dos Dados .....	14
14. Responsabilidade e Sanções.....	14
14.1. A Direção .....	14
14.2. Os Responsáveis pela Proteção de Dados.....	15
14.3. O Encarregado da Proteção de Dados .....	15
15. Derrogações .....	15

16. Glossário .....	16
Responsável pelo Tratamento dos Dados /Responsável /Responsável Conjunto.....	16
Utilizadores de Dados .....	16
Subcontratante .....	16
Titulares de Dados .....	16
Dados Pessoais.....	16
Tratamento .....	17
Categorias Especiais de Dados (p/k/a dados pessoais sensíveis).....	17
Informações anónimas .....	17
Pseudonimização .....	17
IPI ou Informações Pessoais Identificáveis .....	18
ICS ou Informações Confidenciais relativas à Saúde .....	18
IPS ou Informações Pessoais Sensíveis.....	18

## 1. Introdução

Enquanto parte da sua responsabilidade social, a Ipsos declara-se empenhada em cumprir as disposições legislativas, regulamentares e normativas internacionais em matéria de proteção de dados. A presente política de proteção dos dados e da privacidade (“**Política**” ou “**Política de Proteção de Dados**”) aplica-se ao Grupo Ipsos em todo o mundo e assenta em princípios essenciais mundialmente aceites no que diz respeito à proteção de dados. A presente Política adota os princípios fundamentais do Regulamento Geral de Proteção de Dados Pessoais da EU (RGPD) como a norma mínima que deve ser respeitada pelo Grupo Ipsos, assim como pelos seus empregados e fornecedores.

A Ipsos depende da recolha e análise de informação sobre indivíduos (“**Titulares dos Dados**”) para a realização dos seus estudos de mercado e atividades conexas. A fim de manter a confiança dos inquiridos e do público é necessário garantir a proteção dos mesmos contra consequências negativas, riscos ou danos advindos da disponibilização de informação à Ipsos ou do tratamento dado aos seus Dados Pessoais (para a definição e explicação deste termo e de outros termos redigidos com iniciais em maiúsculas, ver o Glossário) pela Ipsos no exercício da sua atividade profissional. A informação em causa pode ser obtida junto de qualquer indivíduo ou organização.

No âmbito das suas atividades, a Ipsos necessita também de proceder à recolha e tratamento de certos tipos de informação sobre as pessoas com quem mantém relações. Entre estas, destacam-se antigos e potenciais empregados, fornecedores, clientes e outros indivíduos com quem deva manter contacto. Além disso, poderá, ocasionalmente, ser forçada por lei a proceder ao tratamento de certos tipos de Dados Pessoais a fim de cumprir determinadas exigências legais.

A presente Política descreve as normas mínimas que deverão ser adotadas no tratamento, recolha, processamento e conservação dos Dados Pessoais com vista a cumprir as regras de proteção de dados da Ipsos.

Os Utilizadores de Dados são obrigados a respeitar a presente Política sempre que procederem ao tratamento de Dados Pessoais em nome e por conta da Ipsos. Qualquer violação da presente Política poderá resultar numa ação disciplinar que poderá incluir o despedimento.

## 2. Âmbito

A presente Política aplica-se a todas as empresas do grupo Ipsos, independentemente da sua localização, e constituirá a norma mínima à qual devem aderir todas as empresas que fazem parte do grupo, assim como os seus empregados e fornecedores, independentemente do facto de o RGPD ter ou não uma aplicação direta a uma atividade ou território específicos.

Todos os que trabalham para a Ipsos têm a responsabilidade de garantir que os Dados Pessoais são adequadamente recolhidos, conservados e tratados.

É da responsabilidade de todos garantir que os Dados Pessoais sejam tratados e processados em conformidade com a presente Política e com os princípios nela estabelecidos em matéria de proteção de dados.

A Ipsos espera também que todos os seus fornecedores/prestadores de serviços respeitem os princípios definidos no presente documento.

## 3. Aplicação de Leis Nacionais e de Códigos de Conduta

A presente Política de Proteção de Dados adota os princípios internacionalmente aceites em matéria de privacidade tal como são definidos no RGPD. Ela é subsidiária e complementar a quaisquer leis nacionais aplicáveis. O direito nacional competente prevalecerá em caso de conflito com a presente Política ou no caso de impor condições mais rigorosas do que a presente Política. Qualquer obrigação de registo, notificação ou informação em matéria de tratamento de dados nos termos da legislação nacional em vigor deve ser observada. O conteúdo da presente Política deve igualmente ser observado na ausência de legislação nacional competente.

Cada uma das empresas do Grupo Ipsos é responsável pelo cumprimento da presente Política de Proteção de Dados e pelas suas obrigações legais aplicáveis. Se houver motivos para crer que as obrigações legais contradizem os deveres que lhes incumbem por força da presente Política de Proteção de Dados, a Empresa em questão deverá informar o Encarregado da Proteção de Dados do país e o Encarregado Geral da Proteção de Dados. Em caso de conflito entre a legislação nacional e a Política de Proteção de Dados, a Ipsos colaborará com a empresa em questão a fim de encontrar uma solução que satisfaça as exigências e os objetivos da presente Política e cumpra com a legislação aplicável.

Além da presente política, a Ipsos subscreve ainda os padrões de conduta do Código Internacional ICC/Esomar para Estudos de Mercado, Opinião, Sociais e Análise de Dados, que pode ser consultado [aqui](#).

## 4. Princípios relativos ao Tratamento de Dados Pessoais

Todos os Dados Pessoais devem ser tratados de forma adequada, independentemente da forma como são recolhidos, registados e processados – em papel, ficheiro informático, base de dados ou registado num outro suporte,

- existindo princípios geralmente aceites destinados a salvaguardá-lo, como as diretrizes da OCDE que regem a [Proteção da Privacidade e a Circulação Transfronteiriça de Dados Pessoais](#) e salvaguardas importantes em diversos estatutos em todo o mundo, incluindo o RGPD.

A Ipsos considera o tratamento lícito e correto dos Dados Pessoais e a manutenção da confiança de todos aqueles com quem se relaciona uma componente vital das suas atividades empresariais e compromete-se a tratar esses Dados Pessoais de forma ética e responsável e em oferecer um nível elevado de segurança e confidencialidade.

Para demonstrar esses compromissos, a Ipsos adota os princípios do RGPD que são, eles próprios, a consagração dos princípios da OCDE. A Ipsos observa os seguintes princípios em matéria de Dados Pessoais, os quais são apresentados de forma mais pormenorizada mais adiante:

- Licitude e lealdade no tratamento.
- Finalidades limitadas e tratamento adequado.
- Tratamento adequado, pertinente e não desproporcionado ao que é necessário relativamente às finalidades.
- Exatidão.
- Conservação apenas durante o período necessário para as finalidades para as quais são tratados.
- Tratamento em conformidade com os direitos do Titular dos Dados.
- Segurança.
- Não transferência para indivíduos ou organizações situados em países terceiros sem a proteção adequada.

### 4.1. Licitude, Lealdade e Transparência

Os Dados Pessoais devem ser recolhidos e tratados com licitude, lealdade e transparência em relação ao Titular dos Dados. Além disso, estes devem ser informados sobre o tipo de tratamento de que são objeto os seus dados. Quando não é este o caso, a base jurídica que justifica o tratamento deve ser documentada. O Responsável pelo Tratamento de Dados competente terá de ser consultado, com vista a decidir se é necessário efetuar uma avaliação do impacto nos dados pessoais (ver também as instruções separadas em matéria de avaliação do impacto nos dados pessoais, disponível na intranet).

### 4.2. Limitação das Finalidades

Os Dados Pessoais apenas devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podem ser tratados de uma forma incompatível com essas finalidades. As alterações subsequentes das finalidades apenas são possíveis de forma limitada, devendo ser fundamentadas e validadas. O Responsável pelo Tratamento de Dados competente terá de ser consultado, com vista a decidir se é necessário efetuar uma avaliação do impacto nos dados pessoais (ver também as instruções separadas em matéria de avaliação do impacto nos dados pessoais, disponível na intranet).

### 4.3. Minimização dos Dados

Os Dados Pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para que são tratados. Deve também ser determinado se e em que medida o tratamento dos Dados Pessoais é necessário para cumprir as finalidades para que são tratados. Sempre que as finalidades o permitirem e sempre que o objetivo visado for proporcional às despesas que envolve, devem ser usados dados anonimizados em vez de Dados Pessoais.

#### **4.4. Exatidão**

Os Dados Pessoais devem ser exatos e, sempre que necessário, atualizados; devem ser adotadas todas as medidas adequadas para garantir que os Dados Pessoais inexatos, tendo em conta as finalidades para que são tratados, são apagados ou retificados sem demora.

#### **4.5. Limitação da Conservação**

Os Dados Pessoais não devem ser conservados de uma forma que permita a identificação dos Titulares dos Dados durante um período que exceda o tempo necessário para cumprir as finalidades para que são tratados. A Ipsos não conservará Dados Pessoais durante períodos mais longos do que os necessários para cumprir a finalidade ou finalidades para que foram recolhidos. A Ipsos adotará todas as medidas adequadas para destruir, ou apagar dos seus sistemas, todos os Dados Pessoais que já não sejam necessários.

#### **4.6. Integridade e Confidencialidade**

Os Dados Pessoais devem ser tratados de uma forma que garanta a sua segurança e proteção contra a sua revelação, divulgação, acesso ou manipulação. Assim, sempre que for metodologicamente possível e sempre que os riscos para os Titulares dos Dados forem proporcionais à despesa que envolvem, devem ser usados dados anonimizados – NOTA: os dados anonimizados são e continuam a ser Dados Pessoais!

#### **4.7. Restrições às Transferências de Dados**

Os Dados Pessoais não devem ser transferidos para países terceiros (nem para outras empresas do grupo Ipsos sediadas nesses países) que, de um modo geral, não ofereçam um nível de proteção adequado (ver também ponto 6 para uma descrição mais pormenorizada), podendo existir países que estabeleçam mais requisitos e/ou requisitos diferentes que devem igualmente ser adotados.

#### **4.8. Medidas e Considerações Gerais**

Para a prossecução das suas atividades na área dos estudos de mercado, a Ipsos subscreve ainda os padrões de conduta do Código Internacional ICC/Esomar para Estudos de Mercado, Opinião, Sociais e Análise de Dados e a Data Protection checklist da Esomar.

### **5. Fundamentos Jurídicos para o Tratamento de Dados**

A Ipsos apenas procederá à recolha, tratamento e utilização de Dados Pessoais nos termos dos seguintes fundamentos jurídicos e desde que os mesmos estejam previstos no direito nacional aplicável. Um destes fundamentos jurídicos será igualmente necessário, se as finalidades originais para que os Dados Pessoais foram recolhidos, tratados e utilizados forem alteradas, salvo existência de uma compatibilidade evidente entre as finalidades originais e as novas finalidades. Ver também ponto 4.2 e novos requisitos de compatibilidade.

## **5.1. Os Dados dos Entrevistados**

Os entrevistados são os Titulares de Dados com quem a Ipsos contacta mais frequentemente no âmbito das suas atividades. Desta forma, assegurar um tratamento adequado aos seus Dados Pessoais é, para a Ipsos, uma preocupação central.

### **5.1.1. O Consentimento para o Tratamento de Dados**

Os Dados Pessoais podem ser tratados com base no consentimento do Titular dos Dados. Antes de dar o seu consentimento, este deve ser informado em conformidade com o princípio da transparência tal como ele é descrito no ponto 4.1. A declaração de consentimento deve ser obtida por escrito ou por meios eletrónicos para efeitos de documentação. Em determinadas circunstâncias, como inquéritos telefónicos, o consentimento pode ser dado verbalmente. Em todos os casos, a concessão da autorização deve ser documentada.

Qualquer consentimento apenas será considerado válido se constituir uma manifestação livre, específica, informada e inequívoca da vontade do Titular dos Dados que, mediante uma declaração ou um ato positivo claro, consente no tratamento dos Dados que lhe digam respeito. Para orientações sobre o consentimento, ver intranet.

### **5.1.2. O Tratamento de Dados no quadro das Relações Contratuais**

Além do consentimento, os seus Dados Pessoais podem ser objeto de tratamento se tal for necessário no contexto de um contrato no qual os Titulares dos Dados sejam parte, com vista a honrar os direitos e as obrigações relevantes, sendo também aplicável sempre que se proceder à celebração ou rescisão de um contrato. Isto aplica-se sobretudo a entrevistados (incluindo os clientes-mistério) que se tornam membros dos painéis da Ipsos.

Em alguns países, a celebração de um contrato é considerada uma forma de consentimento.

### **5.1.3. O Tratamento de Dados de acordo com uma Autorização Legal**

O tratamento de Dados Pessoais também é igualmente permitido mediante solicitação, exigência ou autorização da legislação nacional. Para que o tratamento de dados devidamente autorizado possa efetuar-se é necessário conhecer o tipo e a extensão do tratamento dos dados em causa e cumprir as disposições legais relevantes.

### **5.1.4. O Tratamento de Dados de acordo com os Interesses Legítimos**

Os Dados Pessoais podem ser objeto de tratamento, se tal for necessário para efeito dos interesses legítimos do grupo Ipsos e se existir fundamento jurídico para isso na legislação nacional (p. ex.: RGPD Artº 6º (1) (f)). O interesse legítimo como base para o tratamento de dados não é aceite como fundamento jurídico em todos os países, pelo que prevalecerá a legislação nacional competente. Em geral, as categorias especiais de Dados Especiais não podem ser objeto de tratamento com base no interesse legítimo! Em todo o caso, não é possível proceder ao tratamento de Dados Pessoais com base no interesse legítimo se, no caso em apreço, se comprovar que os interesses do Titular dos Dados são merecedores de proteção e que esta tem precedência. Antes de proceder ao tratamento dos Dados Pessoais com base no interesse legítimo, é necessário confirmar se existe um interesse que merece ser protegido e efetuar uma avaliação do interesse legítimo (na forma de uma avaliação do impacto nos dados pessoais com especial atenção para o interesse legítimo) pela empresa do grupo Ipsos em causa. Esta avaliação deve ser validada pelo Encarregado da Proteção de Dados.

### **5.1.5. O Tratamento de Categorias Especiais de Dados Pessoais**

As categorias especiais de Dados Pessoais apenas podem ser objeto de tratamento se a legislação assim o exigir ou mediante o consentimento explícito do Titular dos Dados. Para mais informações sobre o consentimento, ver intranet. As categorias especiais de Dados Pessoais também podem ser tratadas se tal for considerado obrigatório para fazer valer, exercer ou defender direitos jurídicos. As categorias especiais de Dados Pessoais também podem ser objeto de tratamento no território do EEE se o mesmo for necessário para fins de investigação científica ou histórica e para fins estatísticos (Artº 9 (2) (j)), desde que sujeito a



medidas suplementares adequadas. Antes de aplicar estas disposições, é necessário obter o consentimento do Encarregado da Proteção de Dados.

### **5.1.6. Os Dados dos Utilizadores e a Internet**

Se os Dados Pessoais forem recolhidos, tratados e utilizados em sítios *web* ou em aplicações, o Titular dos Dados deve ser informado numa declaração de privacidade que inclua, quando aplicável, informação sobre testemunhos de conexão (cookies) ou outras medidas técnicas semelhantes. A declaração de privacidade e todas as informações sobre cookies devem estar integradas para que sejam fáceis de identificar, diretamente acessíveis, facilmente assimiláveis e disponíveis para o Titular dos Dados.

No caso de serem criados perfis de utilização (tracking) com vista à avaliação da utilização dos sítios *web* e das aplicações, os Titulares dos Dados devem ser informados desses factos na declaração de privacidade. A localização dos Titulares dos Dados em linha apenas pode ser efetuada se for permitida pela legislação nacional ou mediante o consentimento explícito dos Titulares dos Dados. Mesmo que a localização seja feita com base num pseudónimo do Titular dos Dados, este deverá ter oportunidade de se autoexcluir através do acordo de privacidade. Relativamente ao apuramento de índices de audiência em linha de audiências sem consentimento prévio, a Ipsos adota os princípios promulgados pela [researchchoices.com](http://researchchoices.com).

No caso de acesso aos Dados Pessoais através de sítios *web* ou de aplicações, numa área restringida a utilizadores/entrevistados registados, a identificação e autenticação do Titular dos Dados deverá oferecer proteção suficiente durante o acesso.

No âmbito do compromisso da Ipsos em adotar o Código Esomar, as regras e requisitos definidos em [Guide on Social Media Research](#), [Online Research Guideline](#) e [Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals](#) da Esomar também se aplicam à Ipsos enquanto parte desta política.

## **5.2. Os Dados Pessoais Disponibilizados por Clientes**

A transmissão de Dados Pessoais à Ipsos pelos seus clientes é um facto frequente que tem, geralmente, como objetivo proporcionar-nos uma amostra ou reforçar a amostra existente. No que diz respeito a todos os Dados Pessoais recebidos desta forma, a Ipsos será a entidade responsável pelo seu tratamento, apenas podendo fazê-lo de acordo com as instruções recebidas do cliente ou acordadas com ele. Estas instruções podem incluir restrições em material de transferência de dados para terceiros (entre elas, outras empresas do grupo Ipsos) ou de transferências para países terceiros, assim como requisitos de segurança específicos. Estas restrições devem ser respeitadas. É imperioso que estas instruções sejam documentadas por escrito e acordadas antes que quaisquer disposições contratuais relevantes sejam adotadas pela Ipsos, de modo a garantir que está, de facto, em condições de cumprir as restrições ou requisitos específicos impostos pelos seus clientes.

Independentemente de quaisquer exigências por parte de clientes, todos os Dados Pessoais fornecidos por um cliente:

- a) Apenas podem ser tratados para as finalidades para que foram disponibilizados;
- b) Não podem ser conservados por um período mais longo do que o necessário para cumprir as finalidades para que são tratados;
- c) Estão sujeitos às mesmas exigências de segurança aplicáveis aos Dados Pessoais da própria Ipsos.

## **5.3. Os Dados Pessoais dos Empregados**

### **5.3.1. O Tratamento de Dados no quadro das Relações de Trabalho**

Os Dados Pessoais podem ser objeto de tratamento no quadro das relações laborais, se tal for necessário para iniciar, executar ou rescindir o contrato de trabalho. Quando do início do vínculo laboral, os Dados Pessoais do candidato/a podem ser objeto de tratamento. Se o candidato for rejeitado/a, os seus dados devem ser apagados em conformidade com o período de conservação exigido, salvo se o candidato/a concordar em que os seus dados sejam mantidos em arquivo para futuros processos de seleção. O consentimento é igualmente necessário para a utilização dos dados em futuros processos de seleção antes que a aplicação seja partilhada com outras empresas do grupo Ipsos.

No quadro das relações laborais existentes, o tratamento de dados deve estar sempre relacionado com as finalidades do contrato de trabalho, no caso de não se verificar nenhuma das seguintes circunstâncias em que o tratamento de dados é autorizado.

**Se, no decurso do processo de candidatura, for necessário proceder à recolha de informação sobre um candidate/a junto de terceiros, os requisitos das legislações nacionais correspondentes devem ser observados.** Em caso de dúvida, deverá obter-se o consentimento dos Titulares dos Dados.

O tratamento de Dados Pessoais que esteja relacionado com o vínculo laboral, mas não conste do contrato de trabalho celebrado inicialmente, necessita de uma autorização legal, podendo incluir requisitos legais, regulamentação coletiva com representantes dos empregados, o consentimento dos empregados ou o interesse legítimo da empresa.

### **5.3.2. O Tratamento de Dados de acordo com uma Autorização Legal**

Ver ponto 5.1.3 para outros requisitos.

### **5.3.3. Os Acordos Coletivos e o Tratamento de Dados**

Se uma atividade de tratamento de dados exceder as finalidades de cumprimento de um contrato, pode ser permissível desde que autorizada por um acordo coletivo celebrado entre a entidade empregadora e os representantes dos empregados dentro do âmbito permitido pelo direito laboral. Os contratos devem mencionar a finalidade específica da atividade de tratamento de dados prevista e devem ser redigidos de acordo com os parâmetros da legislação nacional em matéria de proteção de dados e de trabalho.

### **5.3.4. O Consentimento para o Tratamento de Dados**

Os dados dos empregados podem ser objeto de tratamento mediante o consentimento do indivíduo em questão. As declarações de consentimento devem ser apresentadas de forma voluntária. No território da UE/Espaço Económico Europeu, o consentimento não constitui uma base jurídica válida para o tratamento de dados em contexto laboral, dada a existência de uma presunção jurídica de que esse consentimento não foi dado de forma voluntária e de que qualquer tratamento de dados terá de apoiar-se numa das outras bases jurídicas disponíveis. O consentimento involuntário é nulo. Para os casos em que o consentimento for considerado uma base válida para o tratamento de dados, ver ponto 5.1.1 ou outros requisitos. Outra complicação é o facto de o consentimento poder ser retirado, impedindo, assim, o tratamento de dados.

### **5.3.5. O Tratamento de Dados de acordo com os Interesses Legítimos**

Os Dados Pessoais podem ser objeto de tratamento, se tal for necessário para efeito dos interesses legítimos do grupo Ipsos e nos casos em que a legislação aplicável permitir o tratamento de Dados Pessoais com base nos interesses legítimos. Em contexto laboral, os interesses legítimos são, geralmente, de carácter jurídico ou financeiro.

No respeitante aos requisitos e limitações dos interesses legítimos, ver supra, ponto 4.

As medidas de controlo ou de supervisão que exigem o tratamento dos dados dos empregados apenas podem ser adotadas se existir uma obrigação legal ou um motivo legítimo para o fazer. Mesmo existindo um motivo legítimo para o tratamento de dados, a proporcionalidade das medidas de controlo deve ser analisada antes da sua aplicação. Os justificados interesses da empresa para executar as medidas de controlo (p. ex.: cumprimento de regras e procedimentos internos ou interesses em material de segurança) devem ser ponderados face ao interesse que o empregado afetado pela medida possa ter na sua eliminação e que mereça ser protegido, não podendo a medida em causa ser aplicada salvo se for considerada adequada. Os interesses legítimos da empresa e os todos e quaisquer interesses do empregado devem ser identificados e documentados antes da adoção de quaisquer medidas através de uma avaliação de interesses legítimos. Além disso, todas as exigências suplementares ao abrigo da legislação nacional (p. ex.: direitos de codecisão dos representantes dos empregados e direitos à informação dos Titulares de Dados) devem ser tomadas em consideração.

### **5.3.6. O Tratamento de Categorias Especiais de Dados Pessoais**

As categorias especiais de Dados Pessoais apenas podem ser objeto de tratamento se a lei assim o exigir ou se os Titulares dos Dados tiverem dado o seu consentimento explícito. Estes dados também podem ser objeto de tratamento, se tal for obrigatório para fazer valer, exercer ou defender direitos jurídicos.

### **5.3.7. Decisões Automatizadas**

No caso de os Dados Pessoais serem objeto de tratamento automatizado enquanto parte da relação de trabalho e de se proceder à avaliação de informações pessoais específicas tendo em vista uma tomada de decisão (p. ex.: enquanto parte de um processo de seleção de pessoal ou quando da ponderação de classificações), nenhuma decisão que afete negativamente ou produza efeitos adversos no empregado em causa poderá ser tomada exclusivamente com base no tratamento automatizado. A fim de evitar decisões erradas, o tratamento automatizado deverá prever garantias de que o conteúdo da situação é objeto de análise por uma pessoa singular e de que a decisão é tomada com base nesta avaliação. Os Titulares de Dados devem também ser informados dos factos e resultados das decisões individuais automatizadas e do direito de dar resposta.

### **5.3.8. As Telecomunicações e a Internet**

Os equipamentos telefónicos, endereços de correio eletrónico, intranet e internet, juntamente com redes sociais internas, disponibilizados pela Ipsos têm como objetivo principal auxiliar a execução das tarefas relacionadas com a prossecução da sua atividade. São ferramentas de trabalho e fazem parte dos recursos da empresa, podendo ser utilizados nos termos definidos pelas normas legais aplicáveis e as políticas internas da empresa, especialmente a Política Relativa à Segurança da Informação & Utilização Aceitável. No caso de existir uma autorização de utilização para fins pessoais, a mesma deverá estar protegida pelo sigilo das comunicações previsto na legislação nacional competente em matéria de telecomunicações, desde que aplicável.

A Ipsos utiliza tecnologias de filtragem da rede para garantir o cumprimento da sua Política de Utilização Aceitável, da medição e análise de tráfego na internet, e de outras obrigações legais e como defesa contra ataques à sua infraestrutura informática ou utilizadores individuais. Podem ser adotadas medidas de proteção às ligações à rede Ipsos destinadas a bloquear conteúdos tecnicamente prejudiciais e analisar o padrão dos ataques. Por razões de segurança, a utilização de equipamentos telefónicos, endereços de correio eletrónico, intranet/internet e redes sociais internas pode ser trancada permanentemente ou com caráter temporário no caso de endereços/localizações ou tipos de ligação individuais. Os dados pertencentes a indivíduos específicos apenas podem ser avaliados no âmbito de suspeitas concretas e justificadas de violação das normas ou políticas do grupo Ipsos e mediante autorização de uma das pessoas que podem autorizar uma “apreensão legal” (ver também a Política de Gestão da Informação). A legislação nacional relevante deve ser respeitada da mesma forma que os regulamentos do grupo.

## **5.4. Contactos Comerciais**

Em geral, as regras aplicadas aos contactos comerciais, em matéria de proteção da privacidade, não diferem das que são adotadas para os entrevistados. As suas informações de contacto constituem Dados Pessoais, ainda que se refiram a uma estrutura empresarial. Apenas as informações de contacto consideradas verdadeiramente genéricas, não estarão sujeitas a esta Política.

As comunicações comerciais estão, frequentemente, sujeitas a requisitos jurídicos específicos, especialmente se forem feitas por meios eletrónicos ou por telefone.

Deve assumir-se que os contactos comerciais não solicitaram o envio de materiais promocionais, isto é, que os destinatários não pediram para receber comunicações comerciais da Ipsos. Neste caso, e com vista a proceder com toda a legalidade, as condições relativas ao fundamento jurídico, em especial, as exigências de consentimento descritas no ponto 5.1.1 são igualmente aplicáveis.

Um sistema de 'soft opt-in', requerendo a indicação explícita de que se deseja receber correio comercial, pode

ser adotado a título excepcional, desde que se encontre preenchida uma das condições referidas abaixo:

- as informações de contacto do Titular dos Dados tenham sido obtidas no decurso de uma contratação ou de negociações tendo em vista a contratação de serviços prestados pela Ipsos;
- as mensagens se refiram exclusivamente a serviços comerciais semelhantes; e
- é dada ao destinatário uma oportunidade simples de recusar a receção de correio comercial no momento da recolha das suas informações de contacto e, caso não o recuse nesse momento, tenha a possibilidade de bloquear a receção de todas as mensagens futuras de uma maneira simples.

## **6. A Transferência de Dados Pessoais**

A transferência de Dados Pessoais para destinatários dentro e fora do Grupo Ipsos está sujeita aos requisitos de autorização para o tratamento de Dados Pessoais descritos no ponto 4.7 Restrições às Transferências de Dados. Ao destinatário dos dados (seja ele outra empresa do grupo Ipsos ou qualquer subcontratado) deve ser exigida uma utilização dos dados exclusivamente para as finalidades previstas. No que diz respeito às transferências externas, são aplicáveis de maneira cumulativa as disposições referidas neste ponto e no ponto 7 O Tratamento de Dados em Subcontratação/Por Terceiros.

No caso de transferência de Dados Pessoais para um destinatário fora do Grupo Ipsos e de um país terceiro, esse destinatário deverá informar por escrito que mantém um nível de proteção de dados que é equivalente ao descrito na presente Política de Proteção de Dados ou está em conformidade com o que é exigido pela legislação aplicável. Por exemplo, o RGPD define diversos requisitos que devem ser cumpridos antes da ocorrência de qualquer transferência de dados. Isto não se aplica, se a transmissão tiver como base uma obrigação legal. Uma obrigação legal deste tipo pode ter como base a legislação em vigor no país onde está domiciliada a empresa do grupo Ipsos que efetua a transmissão dos dados. Em alternativa, a legislação do país onde está domiciliada a empresa do grupo Ipsos pode aceitar a finalidade para a transmissão dos dados com base nas obrigações legais de um país terceiro.

No caso de transferências de Dados Pessoais por terceiros (p. ex.: um fornecedor de amostras) para uma empresa do grupo Ipsos, deverá ser garantido que os Dados Pessoais em causa podem ser usados para as finalidades previstas.

No caso de transferências de Dados Pessoais de uma empresa do Grupo Ipsos com sede social num determinado país para outra empresa do Grupo Ipsos com sede social num outro país, a empresa que importa os dados está obrigada a cooperar com os inquéritos efetuados pela autoridade de supervisão competente do país onde está localizada a sede social da parte que exporta os dados e a respeitar todas as determinações feitas pela autoridade de supervisão no que se refere ao tratamento dos dados transferidos.

Se um Titular de Dados alegar violação da presente Política de Proteção de Dados por parte de uma empresa do grupo Ipsos localizada num país terceiro que tenha procedido à importação de dados, a empresa do grupo Ipsos responsável pela exportação dos Dados Pessoais compromete-se a apoiar o Titular dos Dados em causa, averiguando os factos e fazendo valer os seus direitos, nos termos da presente Política de Proteção de Dados, contra a empresa do grupo Ipsos responsável pela importação dos dados. Os Titulares de Dados têm ainda direito a fazer valer os seus direitos contra a empresa do grupo Ipsos responsável pela exportação dos dados. No caso de alegações de violação, a empresa responsável pela exportação dos dados deverá apresentar ao Titular dos Dados documentação que comprove que a empresa que importou os Dados Pessoais não violou a presente Política de Proteção de Dados.

As empresas do Grupo Ipsos que transfiram Dados Pessoais para uma empresa do grupo Ipsos localizada num país terceiro serão responsáveis por quaisquer violações da presente Política de Proteção de Dados pela empresa do Grupo Ipsos que receba os Dados Pessoais, como se tivessem elas próprias cometido essa violação.

Todas as transferências de Dados Pessoais efetuadas no seio do Grupo Ipsos apenas serão realizadas depois de o projeto, no âmbito do qual ocorre a transferência, ser devidamente registado no JobBook. Este registo criará um contrato ao abrigo do Ipsos Intragroup Master Services Agreement através do qual as respetivas Cláusulas Modelo da UE serão, automaticamente, aplicáveis à transferência em causa.

## **7. O Tratamento de Dados em Subcontratação/Por Terceiros**

A Ipsos recorre, em muitas situações, a fornecedores externos para o tratamento de Dados Pessoais. Nestes casos, deverá ser celebrado com o fornecedor em causa um contrato de tratamento de dados em nome e por conta da Ipsos. Tal pode ser feito, quer através da

inclusão das disposições adequadas no contrato que rege a relação com o fornecedor na sua globalidade, quer através de um documento específico redigido em separado. No que diz respeito ao tratamento em nome e por conta da Ipsos, o fornecedor só poderá proceder ao tratamento dos Dados Pessoais de acordo com as instruções da Ipsos. A instrução de um fornecedor deve respeitar as seguintes exigências:

- Sempre que os Dados Pessoais em causa se enquadrarem na situação descrita no ponto 5.2 (dados de clientes), deverão ser comunicadas ao fornecedor todas as correspondentes exigências dos clientes.
- A seleção do fornecedor deverá ser feita tendo como base a sua capacidade para cumprir as medidas de proteção exigidas, tanto no plano técnico como no plano organizacional, e de acordo com o processo de aprovação de fornecedores da Ipsos.
- O fornecedor não deverá subcontratar o tratamento de dados sem o prévio consentimento escrito da Ipsos.
- As instruções devem ser comunicadas por escrito por meio de um contrato adequado. As instruções relativas ao tratamento de dados e às responsabilidades da Ipsos e do fornecedor devem ser documentadas.
- Antes do início do tratamento de dados, a Ipsos deve estar segura de que o fornecedor cumprirá as suas obrigações. Os fornecedores podem apresentar uma certificação adequada como forma de documentar o seu cumprimento dos requisitos de segurança de dados. De acordo com o risco do tratamento de dados, as revisões devem realizar-se periodicamente durante o termo de vigência do contrato. A Ipsos pode reservar-se o direito de auditar o cumprimento por parte dos fornecedores.
- No caso de contratos transfronteiriços para o tratamento de dados, devem ser satisfeitos os requisitos nacionais correspondentes em matéria de divulgação dos Dados Pessoais no estrangeiro. Em especial, os Dados Pessoais provenientes do Espaço Económico Europeu podem ser tratados num país terceiro apenas se o fornecedor comprovar um nível de proteção de dados equivalente ao do RGPD e da presente Política de Proteção de Dados. Os seguintes são considerados instrumentos adequados:
  - Um contrato redigido com base nas cláusulas contratuais-tipo da UE dos contratos com fornecedores para o tratamento de dados em países terceiros. Serão exigidos contratos semelhantes para todos os subcontratados pelo fornecedor.
  - Participação do fornecedor num sistema de certificação acreditado pela UE para a atribuição de um nível de proteção de dados suficiente.

## 8. Os Direitos do Titular dos Dados

Todos os Titulares de Dados têm os seguintes direitos. Estes deverão ser imediatamente respeitados pela empresa do grupo Ipsos em causa e não poderão traduzir-se em nenhuma desvantagem para o Titular de Dados. Sempre que a Ipsos proceder ao tratamento de Dados Pessoais nos termos descritos no ponto 5.2 Dados Pessoais fornecidos por Clientes, deverá consultar-se o respetivo contrato assinado com o cliente relativamente ao tratamento a ser feito e o cliente deverá ser imediatamente informado desses direitos.

- **Direito de acesso:**
  - Os Titulares de Dados têm o direito de solicitar informações sobre quais dos seus Dados Pessoais foram conservados, como foram recolhidos e para que finalidades.
  - No caso de os Dados Pessoais serem transferidos para terceiros, o titular dos dados deverá ser informado da identidade do destinatário ou das categorias dos destinatários, incluindo de outras empresas do grupo Ipsos.
- **Direito de Retificação:** No caso de Dados Pessoais incorretos ou incompletos, o Titular dos Dados poderá exigir que os mesmos sejam corrigidos ou completados.
- **Direito de retirar o consentimento:** Sempre que os Dados Pessoais forem objeto de tratamento com base no Consentimento (ver também orientações separadas sobre o Consentimento), os Titulares de Dados terão o direito de se oporem, em qualquer momento, ao tratamento. Estes Dados Pessoais não poderão ser objeto do tratamento que foi contestado.
- **Direito de apagamento.** O Titular dos Dados poderá solicitar que os seus dados sejam apagados, se o seu tratamento não assentar em nenhuma base legal, ou se

esta deixar de ser aplicável. O mesmo é válido se a finalidade subjacente ao tratamento dos dados tiver prescrito ou tiver deixado de ser aplicável por outras razões. Os períodos de conservação existentes e os interesses mercedores de proteção deverão ser respeitados.

- **Direito de oposição:** Os Titulares de Dados têm, em geral, o direito de se opor ao tratamento dos dados que lhes dizem respeito e isto deverá ser tomado em consideração se a proteção dos seus interesses prevalecer sobre os interesses do responsável pelo tratamento devido a uma situação pessoal concreta. Tal não se aplica, se uma disposição legal determinar que os Dados Pessoais são dados a ser tratados.
- **Direito à portabilidade dos dados.** O Titular dos Dados tem o direito de solicitar que os Dados Pessoais que fornece lhe sejam disponibilizados num formato de leitura fácil, como um documento em formato Word ou Excel.

## 9. A Confidencialidade no Tratamento dos Dados

Os Dados Pessoais estão sujeitos ao sigilo. São proibidos a recolha, tratamento ou utilização não autorizada destes dados. O tratamento de dados efetuado por qualquer empregado sem que ele/ela tenha sido autorizado a fazê-lo no âmbito das suas legítimas obrigações é considerado um tratamento não autorizado. Aplica-se o princípio da “necessidade de tomar conhecimento”. Os empregados terão acesso aos Dados Pessoais apenas quando tal for adequado para o tipo e âmbito da tarefa em causa. Isto requer uma divisão e separação cuidadosa, assim como uma limitação, de funções e responsabilidades. Além destes, aplicam-se as disposições relativas à Política de Gestão da Informação.

Os empregados estão proibidos de utilizar os Dados Pessoais para fins pessoais ou comercial, a divulgá-los junto de pessoas não autorizadas, ou a disponibilizá-los de qualquer outra forma. Os supervisores deverão informar os empregados, no início da relação de trabalho, sobre a obrigatoriedade de manter o sigilo de dados. Esta obrigatoriedade manter-se-á em vigor mesmo após o término da relação de trabalho. Os contratos de trabalho celebrados com o pessoal da Ipsos devem conter obrigações de confidencialidade adequadas.

## 10. A Proteção de Dados desde a Conceção e Por Defeito

A Ipsos adotará uma abordagem assente na Proteção de Dados desde a Conceção e Por Defeito em todas as suas atividades e, especialmente, nas seguintes situações:

- construção de novos sistemas informáticos para conservação e acesso a dados pessoais;
- desenvolvimento de novas aplicações ou abordagens de investigação;
- participação numa iniciativa de partilha de dados; ou
- utilização de dados para novos fins.

A Proteção desde a conceção é uma abordagem aos projetos que promove o respeito pela privacidade e a proteção de dados desde o início. Trata-se de uma questão fundamental nas fases iniciais de qualquer projeto e também ao longo do seu ciclo de vida.

A adoção de uma abordagem de proteção desde a conceção é uma medida fundamental para minimizar os riscos para a privacidade e para desenvolver a confiança e a vontade de conceber projetos, processos, produtos ou sistemas, tendo em mente a privacidade desde o primeiro momento.

No que diz respeito aos exemplos referidos acima, o instrumento necessário para garantir o cumprimento do procedimento é a realização de uma Avaliação do Impacto nos dados Pessoais.

## 11. A Segurança do Tratamento

Os Dados Pessoais devem ser protegidos contra a divulgação ou o acesso não autorizados (interna ou externamente), o tratamento ilícito, assim como contra perda, alteração ou



destruição acidentais, independentemente de o seu tratamento ser efetuado por meios eletrónicos ou em papel. Além da segurança dos Dados Pessoais existentes em conformidade com as políticas competentes adotadas pela Ipsos (ver Ipsos Book of Policies and Procedures Capítulo 7, aplicável neste domínio), a introdução de novos métodos de tratamento de dados, em especial novos sistemas informáticos ou abordagens de investigação, deve ser precedida pela definição e adoção de medidas técnicas ou organizacionais que assegurem a proteção dos Dados Pessoais. Estas medidas devem assentar em tecnologia de última geração e ter como base a necessidade de assegurar a proteção dos dados.

Estas medidas técnicas e organizacionais deverão ser estabelecidas em concertação com os responsáveis pela segurança de informação e pela proteção de dados. As medidas técnicas e organizacionais para a proteção de Dados Pessoais fazem parte da Gestão de Segurança da Informação Corporativa e deverão ser ajustadas de forma contínua ao progresso e desenvolvimento técnico e às mudanças organizacionais.

A Ipsos procederá ao tratamento de todos os Dados Pessoais que detém em conformidade com a sua Política de Segurança e tomará as medidas de segurança adequadas contra o tratamento ilícito ou não autorizado de Dados Pessoais e contra a sua perda, alteração ou destruição.

## **12. Auditorias sobre a Proteção dos Dados**

O cumprimento desta Política de Proteção de Dados e a legislação aplicável em matéria de proteção de dados são verificados com regularidade através da realização de auditorias sobre proteção de dados e outras formas de controlo. A realização destes controlos é da responsabilidade do Encarregado da Proteção de Dados, do Auditor Interno e/ou de auditores externos contratados. Vários clientes da Ipsos também têm direito à realização de auditorias ao abrigo dos seus acordos com a Ipsos. Os resultados das auditorias sobre a proteção de dados devem ser comunicados ao Encarregado da Proteção de Dados e ao Responsável pela Conformidade. Mediante solicitação, os resultados das auditorias sobre a proteção de dados serão disponibilizados às autoridades responsáveis pela proteção de dados.

## **13. Incidentes relativos à Proteção dos Dados**

Os empregados devem comunicar, imediatamente, ao seu Encarregado da Proteção de Dados os casos de violação da presente Política de Proteção de Dados ou de outros regulamentos relativos à proteção de Dados Pessoais, em conformidade com o Procedimento de Violação de Dados Pessoais, que pode ser consultado no Capítulo 8 do Ipsos Book of Policies and Procedures. A não comunicação de lacunas graves relativamente aos termos da presente Política podem também ser reportadas ao abrigo do sistema de Denúncias da Ipsos.

Em caso de:

- transferência indevida de Dados Pessoais a terceiros;
- transferência indevida de Dados Pessoais transfronteiras;
- acesso indevido, incluindo por terceiros, a Dados Pessoais ou
- perda de Dados Pessoais (incluindo se caírem em domínio público devido a falhas internas).

Deverá ser feita imediatamente uma notificação de violação de proteção de dados, com vista a assegurar que a) a obrigação de informação ao abrigo de legislação nacional é cumprida, b) os clientes afetados são informados e c) a comunicação entre participantes é gerida. As violações em matéria de Proteção de Dados também constituem um incidente de segurança da informação nos termos da política de Gestão de Incidentes no domínio da Segurança Informática.

## **14. Responsabilidade e Sanções**

### **14.1. A Direção**

Os órgãos executivos das respetivas empresas do Grupo Ipsos são responsáveis pelo tratamento dos dados nas áreas sob a sua responsabilidade. Assim, devem garantir o cumprimento dos requisitos legais em matéria de proteção de dados e dos requisitos contidos na presente Política de Proteção de Dados (p. ex.: e.g. obrigação de informação nacional).

A Direção é responsável por garantir a adoção de medidas organizacionais, técnicas e no plano dos recursos humanos, a fim de que o tratamento de dados seja efetuado em conformidade com estes procedimentos de proteção de dados.

O cumprimento destes requisitos é também responsabilidade dos empregados competentes.

O Encarregado da Proteção de Dados deverá ser informado imediatamente da realização de auditorias sobre a proteção de dados por organismos oficiais. A direção da Ipsos no país em causa deverá comunicar ao Encarregado da Proteção de Dados o nome do Responsável pela Proteção de Dados.

O tratamento incorreto de Dados Pessoais, ou outras violações da legislação relativa à proteção de dados, poderá ser processado criminalmente em muitos países e dar origem a pedidos de indemnização por perdas e danos. As violações que sejam da responsabilidade

individual de empregados podem também resultar na imposição de sanções ao abrigo do direito do trabalho.

## 14.2. Os Responsáveis pela Proteção de Dados

A Ipsos deverá nomear um ou mais Encarregados da Proteção de Dados em todos os países onde se encontra representada. Os Encarregados da Proteção de Dados são as pessoas a contactar, nos planos interno e externo, em matéria de proteção de dados. Poderão efetuar controlos e devem informar os empregados sobre o conteúdo da presente Política de Proteção de Dados e a legislação aplicável. Os elementos da direção competentes deverão prestar assistência ao Encarregado da Proteção de Dados neste domínio. As principais funções do Encarregado da Proteção de Dados são:

- *Informar e aconselhar a organização e os seus empregados sobre a obrigação que lhes incumbe de cumprirem a legislação aplicável em matéria de proteção de dados e a presente Política de Proteção de Dados. Esta tarefa será executada com o apoio e sob a orientação do Grupo e através da rede de Encarregados de Proteção de Dados sob a liderança e formação do Responsável Geral pela Proteção de Dados.*
- *Supervisionar o cumprimento da legislação de proteção de dados, incluindo a gestão de atividades internas em matéria de proteção de dados, prestar aconselhamento (e não realizar) sobre as avaliações do impacto sobre a proteção de dados; formar o pessoal e realizar auditorias internas. Estas tarefas serão executadas com o apoio e a orientação do Grupo. As auditorias, que não sejam investigações pontuais, deverão ser coordenadas com a função de auditoria interna do Grupo.*
- *Ser o primeiro ponto de contacto para as autoridades de supervisão e indivíduos cujos dados sejam objeto de tratamento (empregados, clientes, etc.).*

Em cada um dos países onde a Ipsos se encontra representada, os Encarregados da Proteção de Dados deverão:

- Reportar ao mais alto nível do organograma da organização da Ipsos no país em questão – i.e. aos membros do conselho de administração local.
- Atuar de forma autónoma e independente, não podendo ser despedidos, nem penalizados por exercerem as suas funções.
- Ser dotados dos recursos adequados que lhes permitam cumprir as obrigações que lhes incumbem ao abrigo da legislação aplicável em matéria de proteção de dados e da presente Política de Proteção da Privacidade.

Os Encarregados da Proteção de Dados deverão informar imediatamente o Responsável Geral pela Proteção de Dados sobre a existência de riscos para a proteção de dados.

## 14.3. O Responsável Geral pela Privacidade

O Responsável Geral pela Privacidade, na sua qualidade de elemento autónomo, trabalha para assegurar o cumprimento das diretivas das autoridades reguladoras, nacionais e internacionais, em matéria de proteção de dados. É responsável pela aplicação da presente Política de Proteção de Dados e supervisiona o cumprimento da mesma.

Os Titulares de Dados podem dirigir-se ao Responsável Geral pela Privacidade ou ao Encarregado da Proteção de Dados competente em qualquer momento para manifestar preocupações, fazer perguntas, solicitar informação ou apresentar reclamações relacionadas com a proteção ou segurança de dados. Caso seja solicitado, as preocupações e reclamações serão tratadas com confidencialidade.

No caso de o Encarregado da Proteção de Dados competente não solucionar uma reclamação, nem retificar uma violação da Política de Proteção de Dados, o Responsável Geral pela Privacidade deverá ser consultado imediatamente. As decisões deste último tendo em vista a retificação de violações da proteção de dados deverão ser respeitadas pela direção da empresa em causa. O Responsável Geral pela Privacidade deverá ser sempre informado sobre a realização de inquéritos conduzidos pelas autoridades de supervisão.

## 15. Derrogações

Em casos excepcionais, poderá ser obtida uma derrogação da presente Política, antes de submeter os Dados Pessoais ao tratamento pretendido. Essa derrogação apenas será concedida após a realização de uma avaliação completa do impacto da proteção de dados com vista a determinar e avaliar os riscos para os Titulares de Dados afetados, assim como os riscos legais e o impacto em termos de reputação, estando sujeita à aprovação dos Serviços de Apoio do Presidente da Ipsos.

## 16. Glossário

### Responsável pelo Tratamento dos Dados/Responsável/Responsável Conjunto

Pessoa singular ou organização que determina as finalidades e os meios de tratamento dos Dados Pessoais. Responsável pela definição das práticas e políticas em conformidade com os requisitos legais aplicáveis.

Na maioria dos casos em que a Ipsos receber amostras dos seus clientes, será considerada Responsável Conjunta pelos Dados recolhidos. Isto aplica-se também aos dados recolhidos por nós, mesmo que tenhamos garantido aos entrevistados que as suas respostas serão tratadas com confidencialidade. As responsabilidades e obrigações dos Responsáveis Conjuntos devem ser documentadas e clarificadas por meio de um acordo escrito.

Algumas jurisdições utilizam outras designações para este conceito, como por exemplo **Responsável, Organização, Operador**<sup>1</sup> etc.

### Utilizadores de Dados

Os nossos empregados, cujo trabalho envolve o tratamento de Dados Pessoais. Os utilizadores de Dados devem proteger os dados e os Dados Pessoais que manuseiam de acordo com os termos da presente Política e de todos os procedimentos aplicáveis em matéria de segurança de dados em todos os momentos.

### Subcontratante

Pessoa singular ou organização que não é um Utilizador de Dados que procede ao tratamento de Dados Pessoais em nome e por conta e sob as instruções do Responsável. Os empregados dos responsáveis pelo tratamento dos dados estão excluídos desta definição, mas ela pode incluir fornecedores que manuseiam Dados Pessoais. A Ipsos será Responsável pelo Tratamento dos dados (p. ex. Em relação aos membros do nosso painel ou amostras ad hoc pela Ipsos para participar em inquéritos) ou um Subcontratante (p. ex.: em relação a amostras disponibilizadas por clientes). Algumas jurisdições utilizam outras designações para este conceito, como por exemplo **Terceiro, Intermediário, Operador**<sup>2</sup> etc.

### Titulares dos Dados

Para os efeitos da presente Política, incluem todas as pessoas singulares sobre as quais a Ipsos detém Dados Pessoais. Um Titular de Dados não precisa de ser um nacional do país ou de residir nele. Os Titulares de Dados têm direitos legais relativamente às suas informações pessoais.

### Dados Pessoais

A definição de Dados Pessoais do RGPD (Artº 4º (1)) torna claro o que é entendido por Dados Pessoais e mostra que esta deve ser interpretada de modo lato:

*"...informação relativa a uma pessoa singular identificada ou identificável (titular dos dados)"; é considerada identificável uma pessoa que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".*

Uma pessoa singular é um indivíduo vivo e o RGPD não se aplica a indivíduos já falecidos. No entanto, os estados-membros podem prever regras relativas ao tratamento de Dados Pessoais que digam respeito a indivíduos já falecidos.

As informações relativas a uma empresa são constituem Dados Pessoais.

Deve reconhecer-se que nem sempre é possível saber com absoluta certeza se um elemento individual de informação constitui um Dado Pessoal. Será necessário considerar a totalidade da informação retida sobre o indivíduo em causa ou os meios que poderão ser utilizados para identificar uma pessoa. Com base na evolução constante dos meios tecnológicos, um número crescente de dados passará a ser considerado Dados Pessoais.

---

<sup>1</sup> Singapura

<sup>2</sup> África do Sul

## Tratamento

Uma atividade que envolve a utilização de dados, inclui a recolha, o registo ou a conservação de dados, ou a realização de uma operação ou de um conjunto de operações sobre os dados, tais como a organização, a estruturação, a conservação, a utilização, a divulgação, o apagamento ou a sua destruição. O tratamento também inclui a transferência de Dados Pessoais.

## Categorias especiais de dados (p/k/a dados pessoais sensíveis)

“Categorias especiais de Dados Pessoais” é a nova expressão usada no RGPD, em vez de “dados sensíveis”, a expressão utilizada anteriormente. Estas são agora definidas no Artº 9º do RGPD como dados sobre:

*a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como os dados genéticos [ver abaixo], dados biométricos [ver abaixo] para identificar uma pessoa de forma inequívoca, dados relativos à saúde [ver abaixo] ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*

O RGPD apresenta definições mais completas para algumas destas expressões:

*‘dados genéticos’ Dados Pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta, designadamente, de uma análise de uma amostra biológica proveniente da pessoa singular em causa;*

*‘dados biométricos’ Dados Pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;*

*‘dados relativos à saúde’ Dados Pessoais relacionados com a saúde física e mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;*

## Informações anónimas

Definidas como informações não relacionadas com uma pessoa singular identificada ou identificável, ou com Dados Pessoais tornados anónimos de maneira que o Titular dos Dados deixe de ser identificável (RGPD, Regulamento 26). Devem ser distinguidos de dados que, juntamente com informações suplementares (p. ex., uma chave), possam ser utilizados para identificar uma pessoa singular, sendo então considerados os dados meramente pseudonimizados.

Os dados pseudonimizados continuam a ser abrangidos pela definição de Dados Pessoais, pelo que a eles se aplicam todos os princípios e requisitos do RGPD.

## Pseudonimização

Pseudonimização refere-se ao tratamento de Dados Pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente sujeitas a medidas técnicas e organizativas para assegurar que os Dados Pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. (RGPD Artº 4º (5))

Os dados pseudonimizados referem-se a dados nos quais os elementos identificadores de um conjunto de informações são substituídos por elementos identificadores artificiais, ou por pseudónimos, que são mantidos separadamente e sujeitos a salvaguardas técnicas. Os Dados Pseudonimizados continuam a ser Dados Pessoais, pelo que todos os requisitos relativos à proteção de dados continuam a aplicar-se a eles!!



## **IPI ou Informações Pessoais Identificáveis**

O termo deriva da legislação norte-americana sobre privacidade. Embora, de um ponto de vista prático aplicável à atividade diária desenvolvida pela Ipsos, as expressões Dados Pessoais e IPI possam ser consideradas sinónimas, a utilização da expressão IPI no contexto do RGPD deve ser evitada, pois tem um impacto negativo na nossa obrigação de demonstrar conformidade com o regulamento. Os reguladores são grandes defensores da consistência e exatidão no que se refere à utilização de expressões.

## **ICS ou Informações Confidenciais relativas à Saúde**

Este termo deriva também da legislação norte-americana sobre privacidade, em especial da HIPPA (Health Insurance Portability and Accountability Act de 1996). Embora, de um ponto de vista prático aplicável à atividade diária desenvolvida pela Ipsos, as expressões categorias especiais de Dados Pessoais e IPI devam ser tratadas como sinónimas, a utilização da expressão IPI no contexto do RGPD deve ser evitada.

A questão principal a tomar em consideração neste caso é a de que certos Dados Pessoais que seriam abrangidos pela definição legal de ICS, constituiriam Dados Pessoais e não categorias especiais de dados ao abrigo do RGPD. Por exemplo, o HIPPA consideraria como ICS todas as informações de uma base de dados que RGPD apenas consideraria a orientação sexual como fazendo parte das categorias especiais de Dados Pessoais.

## **IPS ou Informações Pessoais Sensíveis**

Esta expressão encontra-se desatualizada, derivando de legislação anterior. Pode ser considerada sinónimo de "categorias especiais de Dados Pessoais" tal como estas são definidas no RGPD, no seu Artº 9, devendo ser esta a expressão a utilizar. Os reguladores esperam que a Ipsos utilize a terminologia correta demonstrando, assim, a sua conformidade com o regulamento como parte da sua obrigação de responsabilização.

## Documento de Controlo (Art.º 25º RGPD)

Versão	Data	Resumo de Alterações	Autores	Aprovado por
1.0	12.04.2018	Versão aprovada para publicação	Rupert van Hullen	Laurence Stoclet

Revisão dos Documentos	
Data da Última Revisão	12.04.2018
Versão Revista	1.0
Alterações propostas (indicar nº de capítulo e fazer breve descrição das alterações)	N/R
Comissão de Revisão	Encarregado da Proteção de Dados, GC, CIO, MarCom
Entidade/Comissão homologadora	CEO Adjunto & CFO
Data da Próxima Revisão	12.04.2019
Nota: Os registos inseridos nesta tabela não obrigam à alteração do número da versão	