

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (“RGPD”)

Guia de tratamento de dados pessoais no âmbito da atividade das Agências de Viagens e Turismo

*Este documento pretende servir de mero auxiliar no processo de implementação do RGPD e fornecer orientações gerais sem carácter vinculativo. Em caso de dúvida, é aconselhável contactar a Comissão Nacional de Proteção de Dados.

1. RGPD: considerações gerais, conceitos	2
2. Medidas de implementação do RGPD	4
3. Responsável pelo tratamento de dados e subcontratante.....	9
4. Fundamentos legais para tratamento de dados	10
5. Consentimento	11
6. Encarregado de Proteção de Dados (“DPO”)	12
7. Direitos dos titulares dos dados	13
8. Notificações de violações de dados pessoais	16
9. Políticas de Privacidade.....	17
10. Transferências Internacionais	18
11. Marketing direto.....	19
12. Segurança.....	21
13. Coimas.....	21

1. RGPD: considerações gerais, conceitos

A proteção de dados pessoais assume-se atualmente como uma das matérias de maior destaque no seio da União Europeia. O direito à privacidade dos cidadãos e à proteção dos dados de carácter pessoal que lhes dizem respeito, constituem garantias basilares de um Estado de Direito Democrático, cujo cumprimento, em virtude do seu carácter iminentemente pessoal, deve ser assegurado pelos Estados-Membros através do rigoroso cumprimento da legislação aplicável.

Até 2016, a disciplina em matéria de proteção de dados pessoais passava pela aplicação da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, transposta para o ordenamento português pela Lei 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais). Porém, a 27 de abril de 2016 **entrou em vigor o Regulamento n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados – Regulamento Geral sobre a Proteção de Dados (adiante designado “RGPD”) –, trazendo à colação um novo quadro normativo cujas especificidades conduzem à necessidade de adaptação das soluções atualmente adotadas pelas empresas.

O RGPD constitui a alteração mais revolucionária na regulamentação da União Europeia relativa ao tratamento de dados pessoais nos últimos 20 anos. A implementação deste regulamento pretende que o tratamento de dados pessoais seja realizado de forma mais transparente, exata e previsível para os particulares, adaptando o regime jurídico vigente à nova era tecnológica que se vive na atualidade, readquirindo a confiança dos titulares de dados e estimulando o estabelecimento de novas oportunidades negociais no contexto europeu. Os seus objetivos primordiais passam, desta forma, pela *“realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social”*¹.

Diretamente aplicável em todos os Estados Membros a partir do dia 25 de maio de 2018, este novo diploma garante uma proteção competente e eficaz no que

¹ Considerando n.º 2, do RGPD.

diz respeito à proteção das pessoas singulares no tratamento dos seus dados pessoais e à livre circulação dos mesmos, pelo que a adequação a este novo quadro normativo se assume hoje como um dos maiores desafios encarados pelas empresas, designadamente no setor do turismo, onde a prestação de serviços de reservas de viagens impõe e mobiliza a recolha e tratamento de um volume significativo de dados pessoais em contextos transfronteiriços.

De salientar que o RGPD é aplicável a todos os fluxos de dados pessoais detetados no seio das entidades, incluindo, não apenas aqueles que digam respeito ao Cliente, mas também aos colaboradores e outros a que a entidade tenha acesso no âmbito da sua atividade. Não obstante, o presente Guia é direcionado e abrange os aspetos mais relevantes no que diz respeito à relação com o Cliente.

➤ **O que são dados pessoais?**

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

➤ **O que se entende por tratamento de dados pessoais?**

Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como:

- Recolha;
- Registo;
- Organização;
- Estruturação;
- Conservação;

- Adaptação ou alteração;
- Recuperação;
- Consulta;
- Utilização;
- Divulgação por transmissão;
- Difusão ou qualquer outra forma de disponibilização;
- Comparação ou interconexão;
- Limitação;
- Apagamento; ou
- Destruição.

2. Medidas de implementação do RGPD

➤ Conscientização do quadro interno da Agência relativamente ao âmbito, conteúdo e obrigações resultantes do RGPD:

Realização de sessões de formação e esclarecimento direcionadas a todos os colaboradores da Agência, tendo em vista a sua sensibilização quanto ao novo quadro normativo aplicável a partir de 25 de maio e possíveis consequências no caso de incumprimento. É aconselhável que a organização deste tipo de iniciativas permita a todos os colaboradores apreenderem noções gerais e também específicas do RGPD, tendo em conta a estrutura organizacional da Agência e as diversas categorias de funções desempenhadas no exercício da sua atividade.

➤ Mapeamento dos fluxos de dados existentes e conservação de registos de todas as atividades de recolha e tratamento efetuados, por cada base de dados identificada, definindo os seguintes parâmetros:

- (i) Que dados existem e qual a sua natureza;
- (ii) Qual o fundamento legal para a recolha e/ou tratamento dos mesmos;
- (iii) Qual a finalidade do tratamento;

- (iv) Identificação do responsável pelo tratamento;
- (v) Onde se encontram armazenados os dados;
- (vi) Quem são os titulares dos dados e quais as informações que lhes são disponibilizadas;
- (vii) Quem pode aceder aos dados;
- (viii) Quais as medidas de segurança adotadas;
- (ix) Como proceder no caso de ser detetada uma violação de dados;
- (x) Qual o prazo de conservação dos dados.

➤ **Elaboração de Políticas de Privacidade:**

Revisão das Políticas de Privacidade disponibilizadas pela Agência, garantindo a inclusão das informações impostas pelo RGPD e sua disponibilização numa linguagem simples, clara, concisa e de fácil compreensão para o Cliente.

➤ **Revisão de procedimentos internos que permitam o efetivo exercício dos direitos do titular dos dados:**

A Agência deve criar canais de comunicação por forma a garantir, de forma fácil e a título gratuito, dentro de um período de tempo razoável e no prazo máximo de um mês, o efetivo exercício dos direitos que são conferidos aos Clientes por força do RGPD.

➤ **Consentimento:**

Nos casos em que a licitude do tratamento de dados pessoais se baseie no consentimento dos seus titulares, a Agência deve elaborar declarações de consentimento, nos termos da lei, a serem subscritas pelos Clientes, em relação a cada finalidade específica de tratamento. Sempre que o tratamento de categorias especiais de dados (informações que revelem a origem racial ou étnica, crenças religiosas, saúde ou orientação sexual) se revele necessário à execução dos serviços contratados, a Agência apenas pode proceder ao tratamento desses dados caso o Cliente tenha prestado o seu consentimento explícito para o efeito.

➤ **Adotar medidas de segurança adequadas ao cumprimento do RGPD:**

Tendo em conta as técnicas de segurança mais avançadas e o risco que resulta do tratamento dos dados pessoais para os direitos e liberdades do seu titular, a Agência deve adotar sistemas de segurança adequados a esse mesmo risco.

➤ **Implementar sistemas de notificação que permitam informar a autoridade de controlo e/ou o titular dos dados no caso de violação de dados pessoais:**

A Agência deve certificar-se de que adota procedimentos capazes de detetar, denunciar, investigar e comunicar uma violação de dados pessoais à autoridade de controlo e aos respetivos titulares, se aplicável.

➤ **Realizar avaliações de impacto:**

Sem prejuízo da lista de tipos de operações de tratamento sujeitos ao requisito obrigatório de avaliação de impacto que irá ser divulgada pela autoridade de controlo, antes de proceder ao tratamento dos dados pessoais dos Clientes, a Agência deve proceder a uma avaliação de impacto, solicitando parecer prévio ao DPO designado. Desta análise devem constar, pelo menos, os seguintes elementos:

- Descrição sistemática das operações de tratamento previstas no âmbito da atividade desenvolvida pela Agência e qual a finalidade do tratamento e, se aplicável, os interesses legítimos do responsável pelo tratamento;
- Avaliação da necessidade e proporcionalidade das operações de tratamento efetuadas mediante os objetivos esperados;
- Avaliação dos riscos para os direitos e liberdades das pessoas singulares titulares dos dados;

- Identificação das medidas e procedimentos previstos para fazer face a esses riscos e a assegurar a segurança dos dados pessoais dos seus titulares, em conformidade com o RGPD.

Quando a avaliação de impacto determinar que do tratamento previsto resulta um elevado risco para a proteção de dados pessoais, a Agência deve consultar a autoridade de controlo antes de proceder ao respetivo tratamento.

➤ **Rever contratos individuais com entidades subcontratantes:**

Nos casos em que a Agência recorra a entidades subcontratantes no exercício da sua atividade, é-lhe imposta uma avaliação prévia favorável quanto às garantias de execução de medidas técnicas e organizativas pela entidade subcontratante, adequadas ao cumprimento do RGPD. Além disso, estas parcerias devem ser reguladas por contrato, escrito e em formato eletrónico, do qual devem constar disposições que estipulem os seguintes parâmetros:

- (i)** Definição das medidas técnicas e organizativas adequadas ao cumprimento da legislação em vigor em matéria de proteção de dados pessoais, tendo em vista a salvaguarda dos direitos do titular dos dados, anexando ao contrato uma Política de Privacidade e Segurança;
- (ii)** Definição do objeto e duração do tratamento
- (iii)** Natureza e finalidade do tratamento;
- (iv)** Identificação do tipo de dados pessoais objeto de processamento e categorias dos titulares;
- (v)** Obrigações e direitos do responsável pelo tratamento neste âmbito.

Deste contrato deve ainda constar, designadamente, que o subcontratante:

- a)** Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, garantindo a sua vinculação;

- b)** Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a obrigações legais de confidencialidade;
- c)** Adota todas as medidas adequadas à segurança do tratamento e dos dados pessoais do titular;
- d)** Apenas pode proceder à subcontratação de outra entidade nos termos da lei;
- e)** Cooperar e assiste o responsável na resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos que lhes são reconhecidos;
- f)** Apaga/devolve (mediante escolha do responsável) todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, incluindo as cópias de ficheiros (exceto nos casos em que exista disposição legal que imponha a sua conservação);
- g)** Mantém um registo que contenha as informações necessárias para que o responsável possa demonstrar e comprovar o cumprimento das obrigações enunciadas, cooperando com o responsável na realização de eventuais operações de fiscalização;
- h)** Informa o responsável caso, no seu entender, o responsável emitir alguma instrução em violação de disposições legais em matéria de proteção de dados pessoais;
- i)** Cláusula que preveja a extensão das suas obrigações em matéria de proteção de dados no caso de recorrer a outro subcontratante para a realização de operações específicas de tratamento.

➤ **Análise das transferências internacionais de dados pessoais²:**

A Agência terá de garantir de que dispõe de uma base legal para transferir dados pessoais para jurisdições não reconhecidas como tendo regulamentação adequada de proteção de dados pessoais. Essas transferências geralmente irão exigir que o Cliente preste o seu consentimento, especialmente quando estejam em causa categorias especiais

² ECTAA – The European Travel Agents’ and Tour Operators’ Associations - “GDPR Frequently asked questions”.

de dados, designadamente dados de saúde, informações nutricionais ou informações de passaportes.

3. Responsável pelo tratamento de dados e subcontratante

Para efeitos do RGPD, o **responsável** pelo tratamento de dados corresponde à *“pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais”*.

O **subcontratante**, por sua vez, corresponde à *“pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes”*.

O RGPD introduz alterações significativas em matéria de subcontratação, através da introdução de disposições diretamente aplicáveis ao subcontratante e sua responsabilização em caso de incumprimento. O subcontratante trata os dados de forma absolutamente vinculada ao responsável pelo tratamento, estando sujeito às obrigações que decorrem do contrato celebrado entre as partes e a todas aquelas que resultem diretamente da lei.

➤ Qual destes papéis desempenha a Agência?

Dependendo da situação concreta, a Agência pode figurar como responsável pelo tratamento ou entidade subcontratante no tratamento de dados pessoais. Contudo, em regra, como comerciante diretamente em contacto com o Cliente, a Agência figura como responsável pelo tratamento.

➤ E os parceiros comerciais da Agência, como companhias aéreas e hotéis?

Estas entidades também podem figurar como responsáveis pelo tratamento de dados pessoais, uma vez que o RGPD prevê a possibilidade de responsáveis conjuntos pelo tratamento.

Assim, as Agências, na sua relação com estas entidades, devem previamente definir o tipo de relação que terão com as mesmas no âmbito de tratamento e processamento de dados pessoais. As Agências devem ainda informar os Clientes que os seus dados serão processados por entidades terceiras (companhias aéreas, hotéis), fornecendo a sua identidade nas Políticas de Privacidade.

Os GDS's são considerados responsáveis pelo tratamento, para efeitos do Código de Conduta CRS, mas também poderão atuar como subcontratantes para outras finalidades de tratamento de dados.³

4. Fundamentos legais para tratamento de dados

Nos termos do art. 6.º do RGPD, o tratamento de dados neste contexto **só é lícito** caso se verifique, pelo menos, uma das seguintes condições:

- a) Caso o titular dos dados tenha dado o seu consentimento;
- b) O tratamento for necessário para execução de um contrato no qual o titular é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
- c) Cumprimento de uma obrigação jurídica a que a Agência esteja sujeita;
- d) Prossecução de interesses legítimos da Agência ou de terceiros, exceto nos casos em que, mediante ponderação, se conclua pela prevalência dos interesses ou direitos do titular que exijam a proteção dos seus dados. Nos termos do considerando n.º 47 do RGPD, pode ser considerado de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.

³ ECTAA – The European Travel Agents' and Tour Operators' Associations - "*GDPR Frequently asked questions*".

O fundamento legal que legitima o tratamento deve ser aferido de acordo com a finalidade que o tratamento de dados pretende cumprir.

No caso das agências de viagens e turismo e no seu relacionamento com os clientes, deve ser feita uma distinção entre o tratamento de dados efetuado no âmbito da contratação dos serviços solicitados pelo Cliente e, por exemplo, envio de conteúdos de carácter publicitário, pois as finalidades inerentes a este tipo de tratamento são distintas, bem como o fundamento legal que determina a sua licitude.

5. Consentimento

Nos casos em que a licitude do tratamento de dados pessoais dependa da obtenção do consentimento do titular dos dados, para que este consentimento seja considerado válido, deve ser prestado mediante um ato positivo claro, livre, específico, informado e inequívoco. Para que o consentimento seja considerado livre, o Cliente deve encontrar-se efetivamente numa posição de recusar, não sendo admissível colocar a finalização do seu objetivo primário, o da contratação da viagem, na dependência da prestação do seu consentimento para efeitos de fins secundários, como o envio de newsletters ou mensagens de carácter publicitário. Por outro lado, o consentimento não pode ser geral, devendo ser obtido em relação a finalidades perfeitamente especificadas.

Por força da responsabilidade pró-ativa que recai sobre o responsável pelo tratamento por força do RGPD, este tem de se encontrar munido de meios que permitam demonstrar que o titular dos dados efetivamente prestou o seu consentimento para o tratamento dos seus dados pessoais, pelo que devem ser adotadas declarações escritas de consentimento que permitam dar cumprimento às exigências mencionadas, de onde conste expressamente o carácter livremente revogável do mesmo e os meios através dos quais essa revogação pode operar. Para o efeito, o responsável pelo tratamento deve assegurar a existência de canais de comunicação que permitam ao titular dos dados retirar o seu consentimento com igual facilidade com que foi prestado.

O silêncio não vale como consentimento, nem são admissíveis caixas pré-marcadas. Caso as declarações de consentimento prestadas pelo titular dos dados anteriormente à data de aplicação obrigatória do RGPD não cumpram com as novas exigências, estas devem ser revistas e ser obtido novo consentimento em conformidade.

Nos casos que exijam o consentimento de menores, o tratamento de dados pessoais só é lícito mediante autorização dos titulares das responsabilidades parentais da criança.

6. Encarregado de Proteção de Dados (“DPO”)

➤ Funções:

Entidade designada pela Agência, responsável pela supervisão e implementação do RGPD no âmbito da atividade desenvolvida. O DPO deve ser envolvido em todas as questões relacionadas com a proteção de dados pessoais, competindo-lhe, designadamente, as seguintes atribuições:

- a)** Informar e aconselhar o responsável pelo tratamento/subcontratante relativamente às suas obrigações em matéria de proteção de dados;
- b)** Controlar a conformidade das condutas implementadas na entidade mediante as imposições legais em matéria de proteção de dados;
- c)** Cooperar com a CNPD no exercício das suas funções de fiscalização, funcionando como ponto de contacto.

➤ Designação de DPO:

O RGPD dispõe a **obrigatoriedade de designação de um DPO** nos casos em que:

- a) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em **operações de tratamento que, devido à sua**

natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

- b) As atividades do responsável pelo tratamento ou do subcontratante consistam em **operações de tratamento em grande escala de categorias especiais de dados** nos termos do art. 9.º do RGPD.

Face à natureza relativamente indeterminada destes conceitos, no caso das agências de viagens e turismo, por desenvolverem, na maioria dos casos, operações de tratamento que, “devido à sua natureza, âmbito e/ou finalidade” exigem um “controlo regular e sistemático dos titulares dos dados em grande escala” e/ou de “categorias especiais de dados, em larga escala”, será recomendável a designação de um DPO mesmo que, em virtude da situação concreta, se possa concluir pela não obrigatoriedade da sua designação. Em caso de grupos empresariais, o RGPD prevê a possibilidade de ser designado um único DPO desde que “*facilmente acessível a partir de cada estabelecimento*” (n.º 2, art. 37.º RGPD).

A obrigatoriedade desta designação, conforme referido, é, em determinadas situações, uma “zona cinzenta”. Pelo que, devem as Agências ponderar a designação de um DPO, sabendo que a sua existência é uma prova do estrito cumprimento da legislação em causa e, funciona, por isso, como uma salvaguarda para a Agência.

➤ **Perfil profissional aconselhado:**

O DPO deve deter conhecimentos na área jurídica e das tecnologias de informação, preferencialmente com experiência profissional anterior em matéria de proteção de dados pessoais.

7. Direitos dos titulares dos dados

O RGPD prevê um elenco sólido de direitos dos titulares dos dados, dos quais resultam corresponsivos deveres para a Agência:

a) Direito de informação:

O vínculo entre a Agência e o Cliente deve assentar numa relação de transparência. Aquando da recolha dos seus dados pessoais, a Agência deve prestar-lhe o conjunto de informações previsto nos arts. 14.º e 15.º do RGPD, de forma concisa, transparente, perceptível e de facilmente acessível, utilizando uma linguagem clara e simples.

b) Direito de acesso:

Fornecer ao Cliente a confirmação de que os seus dados pessoais se encontram ou não a ser objeto de tratamento, quando solicitada pelo mesmo. Em caso afirmativo, este direito impõe ainda que a Agência permita ao Cliente o acesso a um conjunto de informações, tais como:

- Quais as finalidades do tratamento que está a ser efetuado;
- Categorias dos dados pessoais sujeitos a tratamento;
- Destinatários ou possíveis destinatários dos dados, a quem os mesmos possam ser divulgados;
- Prazo de conservação dos dados ou critérios para a sua fixação;
- Direito de apresentar reclamação junto da autoridade de controlo;
- Informações sobre a forma de obtenção dos seus dados, caso não tenham sido recolhidos junto do Cliente;
- Existência ou não de decisões automatizadas, incluindo a definição de perfis, tal como a lógica subjacente, importância e consequências previstas desse tratamento;
- Quais as garantias oferecidas por países terceiros ou organizações internacionais, quando se verifique a transferência dos seus dados nesses termos.

Este conjunto de informações pode ser fornecido pela Agência, a título gratuito e através de cópia, sem prejuízo dos casos em que o pedido seja efetuado por meios eletrónicos e a informação possa ser fornecida em através dessa mesma via, na ausência de pedido diverso por parte do Cliente.

c) Direito de retificação:

A Agência deve retificar e/ou completar os dados pessoais que digam respeito ao Cliente e que este considere inexatos e/ou incompletos. Esta retificação deve processar-se dentro de um prazo razoável, sem demora injustificada.

d) Direito ao apagamento dos dados, ou a “ser esquecido”:

Ressalvando os casos previstos no n.º 3, do art. 17.º do RGPD, a Agência tem o dever de apagar os dados pessoais do Cliente, sem demora injustificada, a pedido do mesmo, e quando se verificarem as condições previstas na lei.

Em regra, os dados pessoais devem ser conservados pela Agência apenas pelo período de tempo estritamente necessário à prossecução das finalidades que motivaram o seu tratamento, sem prejuízo dos casos em que, em virtude de disposições legais de direito nacional e/ou outros, o seu período de conservação seja diverso.

É essencial que durante esses períodos tais dados sejam mantidos de forma segura. Considerando, porém, que muitas das categorias dos dados de uma reserva (ex.: passaporte, detalhes de pagamento) não são necessários para fins de resolução de litígios ou eventual tratamento de reclamações (por exemplo), devem tais dados ser excluídos assim que deixem de ser necessários para o fim com que foram recolhidos e tratados.

e) Direito à limitação do tratamento:

A Agência deve proceder à limitação do tratamento, caso se aplique uma das situações igualmente previstas na lei.

f) Direito de portabilidade dos dados:

Mediante solicitação do Cliente, a Agência deve fornecer-lhe os dados pessoais que lhe digam respeito, num formato estruturado, de uso corrente e de leitura automática, não podendo a Agência opor-se à transmissão desses mesmos dados a outro responsável pelo tratamento, caso:

- O fundamento legal para o tratamento seja o consentimento ou a execução de um contrato;
- O tratamento seja realizado por meios automatizados.

No exercício deste dever, a Agência deve ainda transmitir diretamente ao potencial responsável pelo tratamento esses mesmos dados caso tal transmissão se revele tecnicamente possível caso o Cliente o solicite.

g) Direito de oposição ao tratamento:

Nos casos em que os dados do Cliente sejam objeto de tratamento para efeitos de prossecução dos interesses legítimos da Agência, o Cliente tem o direito de se opor, a todo o tempo, a esse mesmo tratamento.

Este direito de oposição é-lhe igualmente reconhecido nos casos em que os seus dados sejam tratados para efeitos de comercialização direta e, nos casos em que se verifique a sua oposição, os seus dados pessoais deixam de ser objeto de tratamento para esse fim.

h) Direito de não sujeição a decisões individuais automatizadas, incluindo definição de perfis:

Caso a Agência proceda a tratamentos automatizados, incluindo definição de perfis, tem o dever de fazê-los cessar caso o Cliente não pretenda sujeitar-se a decisões tomadas com base nesse tipo de operação, com exceção dos casos previstos na lei.

8. Notificações de violações de dados pessoais

➤ **O que é uma violação de dados pessoais?**

Qualquer violação de segurança, acidental ou ilícita, da qual resulte:

- Destruição;
- Perda;
- Alteração;

- Divulgação ou acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer tipo de tratamento.

➤ **O que fazer no caso de ser detetada uma violação de dados pessoais?**

A Agência deve notificar a autoridade de controlo, sem demora injustificada e, sempre que possível, até 72h após ter tido conhecimento da mesma, exceto nos casos em que dessa violação não resulte risco para os direitos e liberdades do Cliente.

Sempre que a violação de dados pessoais detetada implique um elevado risco para os direitos e liberdades do Cliente, a Agência deve também proceder à sua notificação, através de linguagem clara e simples, sem demora injustificada.

9. Políticas de Privacidade

Em cumprimento da obrigação de transparência e correspondente direito de informação do qual o titular dos dados pessoais beneficia, a Agência deve elaborar uma Política de Privacidade e fornecê-la ao Cliente logo que se inicie o processo de reserva, v.g. através de links que direcionem o Cliente para o respetivo documento, no caso de reservas *online*. Da Política de Privacidade devem constar as seguintes informações:

- Identidade e contactos do responsável pelo tratamento (se for caso disso, do seu representante);
- Contactos do DPO;
- Finalidades do tratamento;
- Fundamento jurídico do tratamento;
- Quais os interesses legítimos do responsável pelo tratamento/ou terceiros, quando o fundamento legal para o tratamento se baseie nos mesmos;
- Nos casos em que o tratamento seja efetuado com base no consentimento do titular, informar o titular do direito de retirar esse consentimento a qualquer

altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

- Destinatários dos dados pessoais;
- Transferência de dados para um país terceiro/organização internacional;
- Prazo de conservação dos dados ou critérios usados para definir esse prazo;
- Direitos do titular dos dados;
- Direito de apresentar reclamação à CNPD;
- Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato; se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não os fornecer;
- A existência de decisões automatizadas, incluindo definição de perfis e, quando existam, informações úteis quanto à lógica subjacente, importância e consequências previstas de tal tratamento para o titular dos dados.

10. Transferências Internacionais⁴

A atividade desenvolvida pelas agências de viagens e operadores turísticos implica parcerias com entidades não estabelecidas na União Europeia. Nesse sentido, será necessário analisar os relacionamentos mantidos com esses parceiros, apurando, designadamente:

- Qual o fundamento legal que justifica a transferência de dados para essas entidades terceiras;
- Se tal transferência ocorre dentro da UE ou do EEE; e
- Se estas entidades garantem um nível adequado de proteção dos dados pessoais que são transferidos.

Até ao momento, a Comissão determinou que oferecem um nível adequado de proteção, fora do EEE, os seguintes países: Andorra, Argentina, Ilhas Faroe,

⁴ ECTAA – The European Travel Agents’ and Tour Operators’ Associations - “GDPR Frequently asked questions”.

Guernsey, Ilha de Man, Israel, Jersey, Nova Zelândia, Suíça e Uruguai. O Canadá e os EUA também são considerados como tendo níveis adequados de proteção em circunstâncias limitadas (“*Privacy Shield*”).

Quando se verificarem transferências regulares de dados para um fornecedor ou parceiro localizado num país que não disponha de um nível adequado de proteção, é necessário assegurar a adoção de medidas que salvaguardem a segurança dos dados. Para o efeito, nos contratos celebrados com tais entidades, devem ser incluídas cláusulas contratuais-tipo, adotadas pela Comissão ou pela autoridade de controlo. Até ao momento, a Comissão emitiu dois conjuntos de cláusulas contratuais-tipo que podem ser adotadas no caso de transferências de dados de responsáveis situados na UE para responsáveis estabelecidos fora da UE ou do EEE. Emitiu igualmente um conjunto de cláusulas contratuais para transferências de dados entre responsáveis situados na UE para subcontratantes estabelecidos fora da UE ou do EEE, disponíveis no seguinte link: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

Porém, quando as transferências de dados não assumirem um carácter regular, esta operação pode ser efetuada com base no fundamento legal de execução de um contrato ou, no que diga respeito ao tratamento de categorias especiais de dados, com base no consentimento do titular dos dados.

No âmbito das transferências de dados pessoais relativos aos seus clientes individuais para hotéis ou outros parceiros comerciais implicados na organização da estadia desses clientes no estrangeiro, o Grupo de Trabalho do Artigo 29 entende que, nesses casos, as transferências não regulares de dados pessoais podem ocorrer.

11. Marketing direto

Nos termos do considerando n.º 47 do RGPD, a prossecução de interesses legítimos do titular dos dados pode servir de fundamento jurídico a alguns tratamentos de dados pessoais para fins de comercialização direta. Para o efeito, deve ser efetuada

uma ponderação entre esses mesmos interesses (neste caso, interesses comerciais) e os direitos fundamentais da pessoa em causa, da qual não deve resultar a sobreposição destes últimos.

No contexto da relação comercial mantida entre a Agência e o Cliente, deve entender-se como razoável a utilização das suas coordenadas para a oferta de serviços, desde que: (i) essa comercialização se circunscreva ao âmbito da atividade desenvolvida pela Agência; (ii) a informação sobre esta futura utilização dos seus dados seja prestada ao Cliente de forma clara e distinta; e (iii) a Agência garanta explicitamente ao Cliente a possibilidade de **recusar este tipo de tratamento**, de forma gratuita e fácil, a todo o tempo.

No que diz respeito a operações de marketing direto através de comunicações eletrónicas (email, sms e chamadas através de mecanismos automatizados), a utilização dos seus dados pessoais para esta finalidade apenas será lícita caso o titular dos dados tenha prestado previamente o seu consentimento para o efeito⁵.

➤ **O que devem as Agências fazer relativamente às bases de dados de email de Clientes que possuem?**

Tal dependerá da forma como tais dados foram recolhidos. Se os mesmos foram obtidos em virtude de uma relação contratual mantida com a Agência e foi dada ao Cliente a opção de recusar o envio de emails futuros (e tal opção não foi acionada), poderão continuar a utilizá-los ao abrigo da Direta E-Privacy e com base no interesse legítimo previsto no RGPD.

Permitimo-nos, porém, referir, que a posição demonstrada pela CNPD em sessões de trabalho sobre este tema, não é clara, ficando por entender se, ainda que perante

⁵ Considerando n.º 40 da Diretiva 2002/58/CE do Parlamento e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações.

a figura do interesse legítimo, não deverá ser obtido consentimento expresso para efeitos de marketing direto. Não é esse o sentido que retiramos do RGPD, mas não podemos deixar de efetuar esta ressalva.

12. Segurança

O responsável pelo tratamento e, caso aplicável, o subcontratante, devem adotar medidas técnicas e organizativas adequadas a garantir a segurança dos dados pessoais, adaptadas ao tipo de tratamento realizado e ao respetivo risco associado, designadamente:

- Pseudonimização e cifragem dos dados pessoais;
- Medidas que assegurem a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento implementados;
- Capacidade de restabelecer a disponibilidade e acesso aos dados, em tempo útil, no caso de *data breaches*;
- Adoção de processos que testem, apreciem e avaliem, com carácter regular, a eficácia das medidas adotadas tendo em vista a segurança do tratamento.

13. Coimas

O incumprimento das disposições legais em matéria de proteção de dados pode conduzir a Agência a incorrer em coimas até € 20.000,00 ou até 4% do seu volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, consoante o que for mais elevado.