

ASSEMBLEIA DA REPÚBLICA

Lei n.º 21/2019

de 25 de fevereiro

Regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e procede à terceira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna.

A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º da Constituição, o seguinte:

Artigo 1.º

Objeto

1 — A presente lei regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (dados PNR) dos voos provenientes de um Estado-Membro da União Europeia ou de um país terceiro ou com destino a um Estado-Membro da União Europeia ou a um país terceiro, bem como o tratamento desses dados, nomeadamente a sua recolha, utilização e conservação, e o respetivo intercâmbio com os Estados-Membros da União Europeia, transpondo para a ordem jurídica interna a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, e procede à terceira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna.

2 — Os dados PNR recolhidos nos termos da presente lei só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, nos termos previstos nas alíneas a), b) e c) do n.º 2 do artigo 5.º

Artigo 2.º

Definições

Para efeitos da presente lei, entende-se por:

a) «Estado-Membro», Estado-Membro da União Europeia;

b) «País terceiro», Estado que não integra a União Europeia;

c) «Transportadora aérea», uma empresa de transporte aéreo titular de uma licença de exploração válida ou equivalente que lhe permite transportar passageiros por via aérea;

d) «Voo extra-UE», um voo regular ou não regular efetuado por uma transportadora aérea a partir de um país terceiro e programado para aterrar no território nacional, ou a partir do território nacional e programado para aterrar num país terceiro, incluindo, em ambos os casos, os voos com escala no território nacional, no território de um ou mais Estados-Membros ou de países terceiros;

e) «Voo intra-UE», um voo regular ou não regular efetuado por uma transportadora aérea a partir do território de um Estado-Membro e programado para aterrar no território nacional ou a partir do território nacional e programado para aterrar no território de um ou mais Estados-Membros, sem escala no território de um país terceiro;

f) «Passageiro», uma pessoa, incluindo pessoa em trânsito ou em correspondência e excluindo membros da tripulação, transportada ou a transportar numa aeronave com o consentimento da transportadora aérea, decorrendo esse consentimento do registo dessa pessoa na lista de passageiros;

g) «Registo de identificação dos passageiros» ou «PNR» (Passenger Name Record), um registo das formalidades de viagem impostas a cada passageiro que contém as informações necessárias para permitir o tratamento e o controlo das reservas feitas pelas transportadoras aéreas participantes relativamente a cada viagem reservada por uma pessoa ou em seu nome, quer o registo conste dos sistemas de reserva, dos sistemas de controlo das partidas, utilizado para efetuar o controlo dos passageiros embarcados nos voos, ou de sistemas equivalentes que ofereçam as mesmas funcionalidades;

h) «Sistema de reservas», o sistema interno da transportadora aérea, no qual são recolhidos dados PNR para o tratamento das reservas;

i) «Método de transferência por exportação», o método através do qual as transportadoras aéreas transferem os dados PNR enumerados no anexo I à presente lei e da qual faz parte integrante, para a base de dados da autoridade requerente;

j) «Infrações terroristas», as infrações a que se refere a Lei n.º 52/2003, de 22 de agosto, que aprova a lei de combate ao terrorismo, alterada pelas Leis n.ºs 59/2007, de 4 de setembro, 25/2008, de 5 de junho, 17/2011, de 3 de maio, e 60/2015, de 24 de junho;

k) «Criminalidade grave», as infrações enumeradas no anexo II à presente lei e da qual faz parte integrante, puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos;

l) «Anonimizar mediante mascaramento de elementos de dados», tornar invisíveis para os utilizadores os elementos dos dados suscetíveis de identificar diretamente o seu titular.

Artigo 3.º

Gabinete de Informações de Passageiros

1 — É criado o Gabinete de Informações de Passageiros (GIP), como unidade nacional de informações de passageiros, no Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), nos termos e para os efeitos do n.º 6 do artigo 23.º-A da Lei n.º 53/2008, de 29 de agosto, na sua redação atual.

2 — Compete ao GIP, designadamente:

a) A recolha dos dados PNR junto das transportadoras aéreas, pela conservação e pelo tratamento desses dados, bem como pela sua transferência ou pela transferência dos resultados do seu tratamento às autoridades competentes referidas no artigo 7.º;

b) O intercâmbio de dados PNR e dos resultados do tratamento desses dados com as unidades de informações de passageiros de outros Estados-Membros e com a Europol, nos termos dos artigos 8.º e 9.º

3 — O Coordenador do GIP integra o Gabinete de Gestão do PUC-CPI e é nomeado pelos membros do Governo responsáveis pelas áreas da administração interna e da justiça de entre elementos dos órgãos de polícia criminal e dos serviços de segurança sob as respetivas tutelas com competência para a deteção, prevenção e investigação das infrações terroristas e da criminalidade grave, nos termos

e pelo período de tempo previsto no n.º 5 do artigo 23.º-A da Lei n.º 53/2008, de 29 de agosto, na sua redação atual.

4 — O funcionamento do GIP é assegurado por elementos da Guarda Nacional Republicana, da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras e da Autoridade Tributária e Aduaneira, podendo integrar ainda um elemento de ligação da Polícia Marítima, nos termos do n.º 9 do artigo 23.º-A da Lei n.º 53/2008, de 29 de agosto, na sua redação atual.

5 — O GIP é instalado no PUC-CPI, que garante o seu apoio jurídico, técnico e administrativo através dos respetivos serviços de apoio, nos termos dos artigos 4.º e 5.º do Decreto Regulamentar n.º 7/2017, de 7 de agosto, que estabelece a organização e o funcionamento do Ponto Único de Contacto para a Cooperação Policial Internacional.

6 — À composição e à orgânica do GIP aplica-se o artigo 23.º-A da Lei n.º 53/2008, de 29 de agosto, na sua redação atual, e o Decreto Regulamentar n.º 7/2017, de 7 de agosto.

7 — Os procedimentos e soluções tecnológicas adequados para a transferência, tratamento e intercâmbio dos dados PNR, a que se refere o n.º 7 do artigo 13.º, são estabelecidos por portaria do Primeiro-Ministro e dos membros do Governo responsáveis pelas áreas da presidência do Conselho de Ministros, da administração interna, da justiça e do planeamento e infraestruturas, de acordo com a lista dos protocolos comuns e dos formatos de dados reconhecidos, elaborada pela Comissão Europeia, e mediante parecer prévio da Comissão Nacional da Proteção de Dados (CNPD).

8 — A designação dos trabalhadores autorizados a proceder ao tratamento de dados é efetuada por despacho do Secretário-Geral do Sistema de Segurança Interna ou, se necessário, mediante despacho deste e dos membros do Governo de cujas áreas da governação provenham os funcionários a designar.

9 — A formação e a credenciação dos trabalhadores autorizados a efetuar o tratamento de dados são da competência do Coordenador do GIP.

Artigo 4.º

Transferência de dados pelas transportadoras aéreas

1 — As transportadoras aéreas transferem para a base de dados do GIP, pelo método de exportação, os dados PNR dos voos extra-UE e intra-UE enumerados no anexo I, na medida em que tenham recolhido esses dados no exercício normal das suas atividades.

2 — Nos casos em que um voo é explorado por uma ou mais transportadoras aéreas em regime de partilha de código, a obrigação de transferir os dados PNR de todos os passageiros do voo cabe à transportadora aérea que o opera.

3 — Se o voo incluir uma ou mais escalas em aeroportos de diferentes Estados-Membros, as transportadoras aéreas transferem os dados PNR da totalidade dos passageiros para o GIP e para as unidades de informações de passageiros desses Estados-Membros.

4 — Caso tenham recolhido dados referentes a informações prévias sobre passageiros (dados API) a que se refere o n.º 18 do anexo I à presente lei e não os conservem pelos meios técnicos utilizados para os dados PNR, as transportadoras aéreas transferem esses dados para o GIP pelo método de exportação referido no n.º 1.

5 — O disposto na presente lei é aplicável aos dados API transferidos, previstos nos artigos 42.º a 44.º da Lei

n.º 23/2007, de 4 de julho, que aprova o regime jurídico de entrada, permanência, saída e afastamento de estrangeiros do território nacional, alterada pelas Leis n.ºs 29/2012, de 9 de agosto, 56/2015, de 23 de junho, 63/2015, de 30 de junho, 59/2017, de 31 de julho, 102/2017, de 28 de agosto, e 26/2018, de 5 de julho.

6 — Os dados PNR são transferidos com utilização de meios eletrónicos e de protocolos comuns e formatos de dados reconhecidos, adotados de acordo com o procedimento previsto no artigo 5.º do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, e definidos de acordo com a portaria a que se refere o n.º 7 do artigo 3.º da presente lei.

7 — Em caso de avaria técnica, os dados são transferidos por quaisquer outros meios a definir pelo GIP, que assegurem um nível adequado de segurança dos dados.

8 — Os dados PNR são transferidos:

a) 24 a 48 horas antes da hora programada da partida do voo; e

b) Imediatamente após o encerramento do voo, ou seja, logo que os passageiros se encontrem a bordo do avião preparados para partir e o embarque ou desembarque já não seja possível.

9 — No caso referido na alínea b) do número anterior, a transferência pode ser limitada à atualização dos dados transferidos nos termos da alínea a) do mesmo número.

10 — Caso seja necessário aceder aos dados PNR para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou criminalidade grave, as transportadoras aéreas transmitem imediatamente os dados PNR mediante pedido apresentado pelo GIP, independentemente dos prazos de transmissão a que se referem os números anteriores.

Artigo 5.º

Tratamento dos dados PNR

1 — Os dados PNR transferidos pelas transportadoras aéreas são recolhidos pelo GIP numa base de dados destinada a registar, armazenar, manter atualizada e disponibilizar a informação para fins de deteção, prevenção e investigação criminal de infrações terroristas e de criminalidade grave, nos termos previstos na presente lei.

2 — O GIP procede ao tratamento dos dados exclusivamente para as seguintes finalidades:

a) Proceder a uma avaliação dos passageiros antes da sua chegada prevista ao território nacional ou da sua partida prevista do território nacional, a fim de identificar as pessoas que, pelo facto de poderem estar implicadas numa infração terrorista ou numa forma de criminalidade grave, devem ser sujeitas a medidas de polícia, medidas especiais de polícia ou medidas cautelares e de polícia pelas autoridades competentes a que se refere o artigo 7.º e, se for caso disso, pela Europol, nos termos do artigo 9.º;

b) Responder, caso a caso, aos pedidos devidamente fundamentados, baseados em motivos suficientes, apresentados pelas autoridades competentes, para fornecer e tratar dados PNR, em casos específicos, para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas ou da criminalidade grave, e para disponibilizar às autoridades competentes ou, se for caso disso, à Europol, os resultados desse tratamento; e

c) Analisar os dados PNR com o objetivo de atualizar ou criar novos critérios a utilizar no tratamento de dados

nos termos da alínea *b*) do n.º 1 do artigo seguinte, a fim de identificar pessoas que possam estar implicadas em infrações terroristas ou em formas de criminalidade grave.

3 — Se os dados transferidos incluírem dados distintos dos enumerados no anexo I à presente lei, o GIP apaga imediata e definitivamente esses dados assim que os receber.

Artigo 6.º

Avaliação e transmissão dos dados PNR

1 — No âmbito da avaliação dos passageiros a que se refere a alínea *a*) do n.º 2 do artigo anterior, o GIP pode:

a) Comparar os dados PNR com os que constam das bases de dados das forças e serviços de segurança, para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, incluindo bases de dados sobre pessoas ou objetos procurados ou alvo de um alerta, de acordo com as regras aplicáveis a essas bases de dados; ou

b) Proceder ao tratamento dos dados PNR de acordo com critérios preestabelecidos.

2 — Qualquer avaliação dos passageiros de acordo com critérios preestabelecidos, nos termos da alínea *b*) do número anterior, é realizada de forma não discriminatória, não podendo estes critérios, em caso algum, basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual.

3 — Os critérios preestabelecidos são definidos e revisitos regularmente pelo GIP, em cooperação com as autoridades competentes a que se refere o artigo seguinte e com o encarregado de proteção de dados, em função de objetivos específicos, necessários, proporcionais e adequados.

4 — Qualquer resultado positivo obtido através do tratamento automatizado dos dados PNR, nos termos e com a finalidade prevista na alínea *a*) do n.º 2 do artigo anterior, é verificado individualmente por meios não automatizados, para aferir se é ou não necessário que a autoridade competente referida no artigo seguinte intervenha nos termos da lei.

5 — O GIP transmite os dados PNR das pessoas identificadas nos termos da alínea *a*) do n.º 2 do artigo anterior, ou os resultados do tratamento desses dados, às autoridades competentes referidas no artigo seguinte, por sua iniciativa ou a solicitação destas, a fim de serem adotadas medidas de polícia, medidas especiais de polícia ou medidas cautelares e de polícia ou as medidas apropriadas para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, no âmbito das respetivas competências, nos termos da lei processual penal e demais legislação aplicável.

6 — A transmissão de dados só pode ser feita caso a caso e, se houver tratamento automatizado dos dados, após verificação individual por meios não automatizados.

7 — O resultado da avaliação dos passageiros a que se refere a alínea *a*) do n.º 2 do artigo anterior não afeta a entrada em território nacional das pessoas que gozam do direito de livre circulação na União Europeia, sem prejuízo das medidas que, nos termos da lei, devam ser adotadas pelas autoridades competentes, de acordo com o disposto no n.º 5.

8 — Quando a avaliação seja efetuada em relação a um voo intra-UE operado entre Estados-Membros ao qual seja

aplicável o Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016, as consequências de tal avaliação devem observar o referido regulamento.

Artigo 7.º

Autoridades competentes

1 — São autoridades competentes para efeitos de transmissão dos dados PNR ou do resultado do seu tratamento, nos termos e para os fins do n.º 5 do artigo anterior, as entidades policiais e aduaneiras, os serviços de segurança e as autoridades judiciais com competência, nos termos da lei, para a prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

2 — As autoridades referidas no número anterior podem submeter a tratamento ulterior os dados PNR e o resultado do seu tratamento, exclusivamente para efeitos específicos de prevenção, deteção, investigação e repressão das infrações terroristas ou da criminalidade grave.

3 — O disposto no número anterior não prejudica as competências das autoridades policiais, aduaneiras ou judiciais, quando forem detetadas outras infrações ou indícios de outras infrações no decurso de ações desencadeadas na sequência do referido tratamento.

4 — Os dados PNR ou o resultado do seu tratamento que, nos termos e para os efeitos do n.º 1, o GIP deva comunicar às autoridades judiciais, são transmitidos ao Departamento Central de Investigação e Ação Penal.

Artigo 8.º

Intercâmbio de dados e do resultado do seu tratamento entre Estados-Membros

1 — O GIP garante a ligação às unidades de informações de passageiros dos restantes Estados-Membros, assegurando que o intercâmbio de dados PNR, assim como o resultado do seu tratamento, se efetua através do PUC-CPI.

2 — O GIP pode transmitir, por sua iniciativa, às unidades de informações de passageiros de outros Estados-Membros os dados relevantes e necessários, ou o respetivo tratamento, de pessoas identificadas nos termos do disposto no n.º 2 do artigo 5.º

3 — Quando receber dados de pessoas identificadas por uma unidade de informações de passageiros de outro Estado-Membro, no âmbito do tratamento de dados para os fins previstos no n.º 2 do artigo 5.º, o GIP transmite esses dados às autoridades nacionais competentes indicadas no artigo anterior, com conhecimento ao centro operacional do PUC-CPI.

4 — Se necessário, e mediante pedido devidamente fundamentado, o GIP pode solicitar ou transmitir a outra unidade de informações de passageiros dados PNR conservados e ainda não anonimizados, mediante mascaramento de elementos de dados, nos termos do n.º 2 artigo 11.º, bem como o resultado do tratamento desses dados, se este já tiver sido efetuado nos termos da alínea *a*) do n.º 2 do artigo 5.º

5 — O pedido a que se refere o número anterior pode basear-se num elemento de dados ou numa combinação de elementos de dados, consoante o que a unidade de informações de passageiros requerente entenda como adequado no âmbito de um caso específico de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave.

6 — Caso os dados solicitados tenham sido anonimizados mediante mascaramento de elementos de dados, nos termos do n.º 2 do artigo 11.º, o GIP só fornece os dados PNR na íntegra se for razoável considerar que tal é necessário para o fim referido na alínea b) do n.º 2 do artigo 5.º, após autorização da autoridade judiciária competente.

7 — As autoridades competentes indicadas no artigo anterior só podem solicitar diretamente à unidade de informações de passageiros de outro Estado-Membro que lhes forneça dados PNR conservados na sua base de dados se necessário, e em casos de emergência, mediante pedido devidamente fundamentado, remetendo cópia do pedido ao PUC-CPI.

8 — Em circunstâncias excepcionais, quando seja necessário aceder a dados PNR para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com a criminalidade grave, o GIP pode requerer, obter e fornecer a outra unidade de informação de passageiros dados PNR, nos termos do n.º 10 do artigo 4.º, informando a autoridade judiciária competente.

Artigo 9.º

Acesso da Europol aos dados PNR e ao resultado do seu tratamento

1 — A Agência da União Europeia para a Cooperação Policial (Europol) só pode solicitar dados PNR, ou o resultado do seu tratamento, nos limites das suas competências e para o exercício das suas funções.

2 — A Europol pode apresentar, caso a caso, ao GIP, através da Unidade Nacional Europol, um pedido eletrónico devidamente fundamentado de transmissão de dados PNR específicos ou dos resultados do tratamento desses dados.

3 — O pedido pode ser apresentado quando tal for estritamente necessário para apoiar e reforçar a ação dos Estados-Membros na prevenção, deteção ou investigação de uma infração terrorista específica ou de uma forma de criminalidade grave, na medida em que estas estejam abrangidas pelas competências da Europol, nos termos da legislação aplicável.

4 — O pedido indica os motivos razoáveis com base nos quais a Europol considera que a transmissão dos dados PNR ou dos resultados do seu tratamento constitui um contributo substancial para a prevenção, deteção ou investigação da infração penal em causa.

5 — O intercâmbio de informações nos termos do presente artigo efetua-se através da rede SIENA, nos termos da Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, na língua que for aplicável.

Artigo 10.º

Transferência de dados e do resultado do seu tratamento para países terceiros

1 — Os dados PNR e o resultado do seu tratamento que tenham sido armazenados pelo GIP nos termos do artigo seguinte só podem ser transferidos para um país terceiro caso a caso e se:

a) Estiverem preenchidas as condições estabelecidas no regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe

para a ordem jurídica interna a Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016;

b) A transferência for necessária para os fins prosseguidos pela presente lei e referidos no n.º 2 do artigo 1.º;

c) O país terceiro só aceitar transferir os dados para outro país terceiro caso tal seja estritamente necessário para os fins previstos no n.º 2 do artigo 1.º e, se for caso disso, mediante autorização da autoridade judiciária competente; e

d) Estiverem preenchidas as condições estabelecidas nos n.ºs 4 a 6 do artigo 8.º

2 — Quando os dados PNR tenham sido inicialmente obtidos por transmissão de outro Estado-Membro, as autoridades nacionais apenas os podem transmitir a um país terceiro se se verificarem as condições previstas no número anterior e mediante autorização daquele Estado-Membro.

3 — Sem prejuízo do disposto no número anterior e do disposto no regime previsto na alínea a) do n.º 1, a transferência de dados PNR sem autorização prévia do Estado-Membro a partir do qual foram obtidos os dados é permitida em circunstâncias excepcionais se:

a) Essa transferência for essencial para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com criminalidade grave num Estado-Membro ou um país terceiro; e

b) A autorização prévia não puder ser obtida em tempo útil.

4 — Nos casos previstos no número anterior, a autoridade responsável por conceder a autorização para a transferência, nos termos dos n.ºs 4 e 6 do artigo 8.º, é informada sem demora e a transferência é devidamente registada e sujeita a uma verificação posterior.

5 — A transmissão de dados PNR para as autoridades competentes de países terceiros só pode ocorrer em condições compatíveis com o disposto na presente lei e apenas após certificação de que o Estado destinatário os tenciona utilizar de forma compatível com essas condições e salvaguardas, designadamente em matéria de proteção de dados pessoais.

6 — O encarregado de proteção de dados é informado sempre que ocorrer uma transmissão de dados nos termos do presente artigo.

Artigo 11.º

Prazo de conservação e anonimização dos dados

1 — Os dados PNR fornecidos pelas transportadoras aéreas ao GIP são conservados na base de dados a que se refere o n.º 1 do artigo 5.º por um prazo de cinco anos contados a partir da sua transferência, nos termos do artigo 4.º

2 — Decorrido um prazo de seis meses após a transferência, todos os dados PNR são anonimizados, tornando-se invisíveis os seguintes elementos de dados suscetíveis de identificar diretamente o passageiro ao qual dizem respeito:

a) Nome(s), incluindo os nomes de outros passageiros mencionados nos PNR e o número de passageiros nos PNR que viajam em conjunto;

b) Endereço e informações de contacto;

c) Todas as informações sobre os meios de pagamento, incluindo o endereço de faturação, na medida em que contenham informações suscetíveis de identificar diretamente o passageiro ao qual os PNR dizem respeito ou quaisquer outras pessoas;

d) Informação de passageiro frequente;

- e) Observações gerais, na medida em que contenham informações suscetíveis de permitir identificar diretamente o passageiro ao qual os PNR dizem respeito; e
f) Quaisquer dados API que tenham sido recolhidos.

3 — Decorrido o prazo de seis meses referido no número anterior, só é permitida a divulgação de dados integrais PNR caso essa divulgação seja:

a) Considerada necessária, com base em motivos razoáveis, para os fins referidos na alínea b) do n.º 2 do artigo 5.º; e

b) Se for caso disso, autorizada pela autoridade judiciária competente.

4 — Os dados PNR são apagados de forma definitiva no termo do prazo referido no n.º 1, sem prejuízo dos casos em que dados PNR específicos tenham sido transferidos para uma autoridade competente e sejam utilizados no âmbito de um caso concreto para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave, caso em que a conservação dos dados pela autoridade competente se rege pela lei processual ou de proteção de dados pessoais que lhe for aplicável.

5 — O resultado do tratamento a que se refere a alínea a) do n.º 2 do artigo 5.º só é conservado pelo GIP durante o período necessário para informar as autoridades competentes e as unidades de informações de passageiros de outros Estados-Membros, nos termos do artigo 8.º

6 — Caso se constate, na sequência de uma verificação individual por meios não automatizados, nos termos do n.º 4 do artigo 6.º, que o resultado do tratamento automatizado é negativo, este pode, ainda assim, ser conservado a fim de evitar falsos resultados positivos no futuro, desde que os dados que lhe serviram de base não sejam apagados nos termos do n.º 4.

Artigo 12.º

Proteção de dados pessoais

1 — Ao tratamento de dados pessoais nos termos da presente lei aplica-se o disposto no regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, nomeadamente quanto ao direito de acesso, retificação, apagamento e limitação, direito a indemnização e a recurso judicial, confidencialidade do tratamento e segurança dos dados.

2 — O disposto no número anterior não prejudica a aplicação do Regulamento Geral sobre a Proteção de Dados, aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ao tratamento de dados pessoais pelas transportadoras aéreas, especialmente no que se refere às suas obrigações de tomarem as medidas técnicas e organizativas adequadas para proteger a segurança e confidencialidade dos dados pessoais.

3 — É proibido o tratamento de dados PNR que revelem a raça ou origem étnica da pessoa, as suas opiniões políticas, religião ou convicções filosóficas, filiação sindical, saúde, vida ou orientação sexual.

4 — Se receber dados PNR que revelem as informações a que se refere o número anterior, o GIP procede ao seu apagamento imediato.

5 — Ao tratamento, pelas autoridades competentes, de dados PNR transferidos para essas entidades, a que se refere o artigo 7.º, é aplicável o disposto na lei processual penal e no regime jurídico referido no n.º 1.

Artigo 13.º

Controlo do tratamento de dados PNR

1 — O GIP conserva a documentação relativa a todos os sistemas e procedimentos de tratamento de dados sob a sua responsabilidade, incluindo, pelo menos:

a) O nome e os contactos da organização e do pessoal do GIP a quem é confiado o tratamento de dados PNR e os diferentes níveis de autorização de acesso;

b) Os pedidos apresentados pelas autoridades competentes, pelas unidades de informações de passageiros de outros Estados-Membros e pela Europol;

c) Todos os pedidos e transferências de dados PNR para um país terceiro.

2 — O PUC-CPI conserva cópia da documentação relativa às alíneas b) e c) do número anterior.

3 — O GIP conserva, pelo menos, registos da recolha, consulta, divulgação e apagamento dos dados.

4 — Os registos das operações de consulta e de divulgação indicam, em especial, a finalidade, a data e a hora dessas operações, a identidade da pessoa que consultou ou divulgou os dados PNR e, se possível, o destino da informação, incluindo a identidade dos seus destinatários.

5 — Os registos e os documentos a que se referem os números anteriores só podem ser utilizados para efeitos de verificação e de autocontrolo, para garantir a integridade e a segurança dos dados e para efeitos de auditoria.

6 — O GIP disponibiliza a documentação e os registos referidos nos números anteriores à autoridade de controlo, a pedido desta.

7 — Os registos a que se referem os n.ºs 2 e 3 são conservados durante um prazo de cinco anos.

8 — O GIP adota e aplica as medidas técnicas e de organização e os procedimentos adequados para garantir um elevado nível de segurança, adaptado aos riscos que o tratamento representa e à natureza dos dados PNR.

9 — Em caso de violação de dados pessoais que seja suscetível de resultar num elevado risco para a proteção dos dados ou de prejudicar a privacidade do seu titular, o GIP comunica tal facto ao titular dos dados e à autoridade nacional a que se refere o artigo seguinte, sem demora injustificada.

Artigo 14.º

Autoridade de controlo

A fiscalização da aplicação da presente lei compete à CNPD, enquanto autoridade de controlo a que se refere o regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Artigo 15.º

Responsável pela proteção de dados

O Coordenador do GIP é o responsável pelo tratamento de dados PNR a que se refere a presente lei.

Artigo 16.º

Encarregado de proteção de dados

1 — O Coordenador do GIP designa um encarregado de proteção de dados, incumbido de controlar o tratamento de dados PNR e de aplicar as salvaguardas relevantes.

2 — À designação, cargo e funções do encarregado de proteção de dados é aplicável o disposto no regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3 — O encarregado de proteção de dados é o ponto de contacto único dos titulares dos dados, que têm o direito de o contactar para todos os assuntos respeitantes ao tratamento de dados PNR.

4 — O encarregado de proteção de dados tem acesso a todos os dados tratados pelo GIP, remetendo o caso para a autoridade de controlo quando considerar que o tratamento de dados não foi efetuado em conformidade com a lei.

Artigo 17.º

Protocolos comuns e formatos de dados reconhecidos

1 — As transferências de dados a que se refere o artigo 4.º são efetuadas por meios eletrónicos que ofereçam garantias suficientes de segurança no que respeita às medidas técnicas e de organização aplicáveis ao tratamento dos dados.

2 — Um ano após a adoção pela Comissão Europeia dos protocolos comuns e dos formatos de dados reconhecidos, todas as transferências de dados PNR pelas transportadoras aéreas para o GIP passam a ser efetuadas eletronicamente através de métodos seguros conformes com esses protocolos comuns.

3 — Os dados PNR são transferidos num formato de dados reconhecido, a fim de assegurar a sua legibilidade por todas as partes envolvidas.

4 — As transportadoras aéreas são obrigadas a seleccionar e a identificar junto do GIP o protocolo comum e o formato de dados que tencionam utilizar para as suas transferências.

5 — É aplicável o disposto no n.º 1 enquanto os protocolos comuns e os formatos de dados reconhecidos não estiverem disponíveis.

Artigo 18.º

Sigilo profissional

1 — Os responsáveis pelo tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais recolhidos, transferidos ou tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

2 — A violação do dever de sigilo é punida nos termos previstos no artigo 383.º do Código Penal.

Artigo 19.º

Violação das obrigações impostas às transportadoras aéreas

1 — As transportadoras que não tenham transferido os dados PNR a que estão obrigadas de acordo com o artigo 4.º ou que os tenham transmitido de forma incorreta, incompleta, falsificada ou após o prazo, são punidas, por cada viagem, com coima de 20 000 € a 100 000 €.

2 — Se for efetuada em formato diferente do requerido nos termos do n.º 5 do artigo 4.º e do artigo 17.º, a transferência é punível com coimas de 10 000 € a 50 000 €.

3 — A negligência é punível.

4 — A aplicação das coimas é da competência do Serviço de Estrangeiros e Fronteiras.

5 — O produto das coimas reverte em 60 % para o Estado e em 40 % para o Serviço de Estrangeiros e Fronteiras.

6 — É subsidiariamente aplicável o disposto no regime geral do ilícito de mera ordenação social.

7 — O não cumprimento da obrigação de transferência de dados API indicados no n.º 18 do anexo I, a efetuar conjuntamente com os restantes dados PNR, é sancionado somente nos termos dos artigos 42.º a 44.º e 196.º da Lei n.º 23/2007, de 4 de julho.

Artigo 20.º

Violação das disposições relativas à proteção de dados pessoais

À violação das disposições relativas à proteção de dados pessoais aplica-se o regime contraordenacional previsto no regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Artigo 21.º

Comunicação de dados estatísticos

1 — São anualmente comunicadas à Comissão Europeia as seguintes informações sobre os dados PNR comunicados ao GIP:

a) Número total de passageiros cujos dados PNR foram objeto de recolha e de intercâmbio;

b) Número de passageiros identificados sujeitos a medidas de polícia, medidas especiais de polícia ou medidas cautelares e de polícia.

2 — As informações a que se refere o número anterior não podem incluir dados pessoais.

Artigo 22.º

Alteração à Lei n.º 53/2008, de 29 de agosto

O artigo 23.º-A da Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, alterada pela Lei n.º 59/2015, de 24 de junho, e pelo Decreto-Lei n.º 49/2017, de 24 de maio, passa a ter a seguinte redação:

«Artigo 23.º-A

[...]

- 1 —
2 —

- 3 —
 4 —
 5 —
 6 — O PUC-CPI reúne, sob a mesma gestão, o Gabinete Nacional Sirene, o Gabinete Nacional da Interpol, a Unidade Nacional da Europol, a coordenação dos oficiais de ligação nacionais e estrangeiros, a coordenação dos Centros de Cooperação Policial e Aduaneira, os pontos de contacto decorrentes das Decisões Prüm e o Gabinete de Informações de Passageiros.
 7 —
 8 —
 9 —
 10 —
 11 —
 12 —»

Artigo 23.º

Alteração ao anexo à Lei n.º 53/2008, de 29 de agosto

O anexo à Lei n.º 53/2008, de 29 de agosto, passa a ter a seguinte redação:

«Mapa de pessoal dirigente

Designação de cargos dirigentes	Número de lugares
Coordenador de Gabinete	5

Artigo 24.º

Entrada em vigor e produção de efeitos

A presente lei entra em vigor no dia seguinte ao da sua publicação, produzindo efeitos com a entrada em vigor do regime jurídico relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Aprovada em 7 de dezembro de 2018.

O Presidente da Assembleia da República, *Eduardo Ferro Rodrigues*.

Promulgada em 11 de fevereiro de 2019.

Publique-se.

O Presidente da República, **MARCELO REBELO DE SOUSA**.

Referendada em 15 de fevereiro de 2019.

O Primeiro-Ministro, *António Luís Santos da Costa*.

ANEXO I

Dados dos registos de identificação dos passageiros (dados PNR) recolhidos pelas transportadoras aéreas a que se refere o artigo 4.º

- 1 — Código de identificação do registo PNR.
 2 — Data da reserva/emissão do bilhete.
 3 — Data(s) da viagem prevista.
 4 — Nome(s).

5 — Endereço e informações de contacto (número de telefone, endereço de correio eletrónico).

6 — Todas as informações sobre as modalidades de pagamento, incluindo o endereço de faturação.

7 — Itinerário completo para o PNR em causa.

8 — Informação de passageiro frequente.

9 — Agência/agente de viagens.

10 — Situação do passageiro, incluindo confirmações, situação do registo, não comparência ou passageiro de última hora sem reserva.

11 — Informação do PNR separada/dividida.

12 — Observações gerais, designadamente todas as informações disponíveis sobre menores não acompanhados com idade inferior a 18 anos, como nome e sexo do menor, idade, língua(s) falada(s), nome e contactos da pessoa que o acompanha no momento da partida e sua relação com o menor, nome e contactos da pessoa que o acompanha no momento da chegada e sua relação com o menor, agente presente na partida e na chegada.

13 — Informações sobre a emissão dos bilhetes, incluindo número dos bilhetes, data de emissão, bilhetes só de ida, dados ATFQ (Automatic Ticket Fare Quote).

14 — Número do lugar e outras informações relativas ao lugar.

15 — Informações sobre a partilha de código.

16 — Todas as informações relativas às bagagens.

17 — Número e outros nomes de passageiros que figuram no PNR.

18 — Todas as informações prévias sobre os passageiros (dados API) que tenham sido recolhidas, incluindo tipo e número de documento(s), país de emissão e termo de validade do(s) documento(s), nacionalidade, nome(s) e apelido(s), sexo, data de nascimento, companhia aérea, número de voo, data de partida, data de chegada, aeroporto de partida, aeroporto de chegada, hora de partida e hora de chegada.

19 — Historial completo das modificações dos dados PNR enumerados nos números anteriores.

ANEXO II

Lista de infrações a que se refere a alínea k) do artigo 2.º

- 1 — Participação em associação criminosa.
 2 — Tráfico de seres humanos.
 3 — Exploração sexual e pedopornografia.
 4 — Tráfico de estupefacientes e substâncias psicotrópicas.
 5 — Tráfico de armas, munições e explosivos.
 6 — Corrupção.
 7 — Fraude, incluindo a fraude lesiva dos interesses financeiros da União, na aceção da Convenção de 26 de julho de 1995, relativa à Proteção dos Interesses Financeiros das Comunidades Europeias.
 8 — Branqueamento dos produtos do crime e contrafação de moeda, incluindo o euro.
 9 — Criminalidade informática e cibercrime.
 10 — Crimes contra o ambiente, incluindo o tráfico de espécies animais ameaçadas e de espécies e variedades vegetais ameaçadas.
 11 — Auxílio à entrada e à permanência irregulares.
 12 — Homicídio voluntário, ofensas à integridade física graves.
 13 — Tráfico de órgãos e tecidos humanos.
 14 — Rapto, sequestro e tomada de reféns.
 15 — Furto ou roubo organizado ou à mão armada.

16 — Tráfico de bens culturais, incluindo antiguidades e obras de arte.

17 — Contrafação, imitação e uso ilegal de marca.

18 — Falsificação de documentos administrativos e respetivo tráfico.

19 — Tráfico de substâncias hormonais e de outros estimuladores de crescimento.

20 — Tráfico de materiais nucleares e radioativos.

21 — Violação.

22 — Crimes abrangidos pela jurisdição do Tribunal Penal Internacional.

23 — Desvio de avião ou navio.

24 — Sabotagem.

25 — Tráfico de veículos furtados ou roubados.

26 — Espionagem industrial.

112079533

PRESIDÊNCIA E DA MODERNIZAÇÃO ADMINISTRATIVA E FINANÇAS

Portaria n.º 68/2019

de 25 de fevereiro

O Instituto Nacional de Estatística, I. P. (INE, I. P.), tem prosseguido a estratégia de reforçar a produção estatística através da apropriação de um vasto conjunto de dados administrativos. O recurso a dados administrativos para fins estatísticos permite a substituição gradual dos modos de recolha direta pela utilização de informação administrativa, permitindo reduzir os custos de contexto junto dos respondentes, cidadãos, empresas e outras entidades, bem como aumentar a qualidade e a eficiência dos processos de produção estatística do INE, I. P.

Em complemento do trabalho desenvolvido, as novas exigências de informação ditam a necessidade de fortalecer a capacidade de gestão e de análise de dados da Administração Pública. O desenvolvimento da Infraestrutura Nacional de Dados no INE, I. P., visa responder ao referido desafio, assente em melhor informação estatística, maior capacidade analítica e flexibilidade de adequação da informação às necessidades da tomada de decisão.

Neste âmbito, torna-se necessário proceder a ajustamentos na organização interna do Instituto, nomeadamente no que respeita às competências do Departamento de Metodologia e de Sistemas de Informação e do Departamento de Recolha de Informação, cuja designação importa alterar. Paralelamente, cumpre definir o estatuto remuneratório da função de encarregado de proteção de dados. A referida função assume especial responsabilidade, complexidade e especificidade no contexto da missão e das atribuições prosseguidas pelo INE, I. P., características necessariamente acentuadas com o desenvolvimento da Infraestrutura Nacional de Dados. Com efeito, o encarregado de proteção de dados zela pela segurança dos dados, garantindo a confiança não apenas dos respetivos titulares, mas também de todos os intervenientes externos a quem o INE, I. P., fornece soluções de recolha ou de armazenamento de informação.

Assim:

Ao abrigo do artigo 12.º da Lei n.º 3/2004, de 15 de janeiro, manda o Governo, pela Ministra da Presidência

e da Modernização Administrativa e pelo Ministro das Finanças, o seguinte:

Artigo 1.º

Alteração

Os artigos 1.º, 6.º e 7.º do anexo à Portaria n.º 423/2012, de 28 de dezembro, alterada pela Portaria n.º 120/2014, de 9 de junho, que aprovou os estatutos do Instituto Nacional de Estatística, I. P., passam a ter seguinte redação:

«Artigo 1.º

[...]

- 1 —
- 2 —
- a)
- b)
- c)
- d) Departamento de Recolha e Gestão de Dados;
- e)
- f)
- g)

- 3 —
- 4 —
- 5 —
- 6 —
- 7 —

8 — O INE, I. P., dispõe de um encarregado de proteção de dados, designado pelo conselho diretivo, que coordena a matéria relativa aos dados pessoais e ao qual é aplicável o disposto no n.º 3 do artigo 11.º considerando a natureza e complexidade das respetivas funções.

Artigo 6.º

Departamento de Metodologia e de Sistemas de Informação

Ao Departamento de Metodologia e de Sistemas de Informação, abreviadamente designado por DMSI, compete:

a) Investigar, estudar e propor métodos estatísticos, no domínio económico e social, para a produção e disponibilização de estatísticas oficiais e para a integração de novas fontes de dados;

b) Gerir e manter atualizado o sistema de metainformação estatística, nomeadamente, através da harmonização com as classificações e conceitos, de acordo com as definições europeias e internacionais;

c) Certificar tecnicamente as operações estatísticas oficiais;

d) Realizar o registo prévio dos suportes de recolha a utilizar na produção das estatísticas oficiais;

e) Assegurar a gestão, manutenção e coordenação das infraestruturas de unidades estatísticas e de dados geográficos;

f) Aplicar a legislação europeia relativa ao estabelecimento de uma infraestrutura de informação geográfica na União Europeia, concretizando as disposições de execução relativas à harmonização dos conjuntos de dados geográficos e disponibilização de serviços;

g) Assegurar a gestão, manutenção e coordenação das infraestruturas de dados, para a integração de diferentes