GRUPO ELIOR

Política de proteção de dados pessoais

Âmbito	Todos os âmbitos
Versão	V1
Responsável pela redação	Comité operacional para os DP
Responsável pela validação	Comité diretivo para os DP
Data de publicação	01/03/2019
Data de atualização	

Introdução

A presente política de proteção de dados pessoais define a forma como o Grupo Elior procede à aplicação do tratamento de dados pessoais para garantir a proteção dos direitos e das liberdades fundamentais das pessoas singulares e, nomeadamente, o seu direito à proteção de dados pessoais.

A política define as normas que todos os colaboradores, colaboradoras, parceiros e subcontratantes do Grupo Elior devem cumprir quando tratam os dados pessoais.

Recorda-se que o incumprimento das obrigações relativas à proteção de dados pessoais expõe o Grupo Elior a uma sanção de 4 % do seu volume de negócios mundial; a título indicativo, isso representa cerca de 268 milhões de euros com base nos resultados do encerramento do exercício, em 30 de setembro de 2018.

Cada um dos titulares dos dados deve, nomeadamente, garantir que:

- cumpre o princípio de proteção da privacidade desde a conceção (*privacy by design*) de novos projetos e, nomeadamente, que cada tratamento de dados (i) corresponde a uma finalidade delimitada, (ii) prevê informar as pessoas do tratamento de dados aplicado, (iii) determina medidas de proteção e (iv) fixa um prazo de conservação dos dados pessoais;
- cumpre os prazos impostos relativamente à resposta aos pedidos de exercício dos direitos, ou seja, um mês, e à notificação de qualquer fuga de dados às autoridades competentes no prazo de 72 horas;
- de uma forma mais geral, cumpre os processos e as recomendações aplicados pela presente política e à solicitação, se for caso disso, dos embaixadores da proteção de dados pessoais ou da equipa do RGPD (Regulamento Geral de Proteção de Dados) do Grupo Elior através do endereço gdpr-contact@eliorgroup.com.

Glossário

«Grupo Elior» designa a empresa Elior Group e todas as empresas que, na aceção do artigo L233-3 do Código Comercial,

(i) estão sob o seu controlo direto ou indireto da empresa Elior Group, ou,
(ii) estão, direta ou indiretamente, sob o controlo comum com a empresa Elior Group;

«Dado(s) pessoal(ais)» ou **«DP»** designa qualquer informação relativa a uma pessoa singular identificada ou identificável (a seguir designada **«titular dos dados»**); É considerada uma **«pessoa singular 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;

«**Tratamento de dados**» designa qualquer operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição;

«Responsável pelo tratamento» designa a 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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União Europeia ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação que podem ser previstos pelo direito da União Europeia ou de um Estado-Membro;

«Subcontratante» designa uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

«Responsável pelo sistema de informação» designa o colaborador no Grupo Elior, garante do conhecimento técnico relativo aos recursos informáticos envolvidos no tratamento, e isto para cada tratamento de DP identificado no Grupo Elior;

«Responsável técnico pelo tratamento» designa o colaborador no Grupo Elior, que define a necessidade técnica e os objetivos (gestão de projetos) do tratamento, e isto para cada tratamento de dados identificado no Grupo Elior;

«**Destinatário**» designa a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um destinatário exterior ao Grupo Elior (terceiro). No entanto, as autoridades públicas suscetíveis de receber comunicações de dados pessoais no âmbito de uma missão de inquérito específica não são consideradas destinatárias; o tratamento de dados pessoais por estas autoridades está em conformidade com as regras aplicáveis em matéria de proteção de dados em função das finalidades do tratamento;

«Consentimento» [do titular dos dados] designa uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

«Violação de dados pessoais» significa uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

«Regras vinculativas aplicáveis à empresa» ou «**Binding Corporate Rules**» ou «**RVE**» designa uma política de proteção de dados intra-Grupo no âmbito de qualquer transferência de dados pessoais que ocorra total ou parcialmente fora do Espaço Económico Europeu. São juridicamente vinculativas e cumpridas pelas entidades signatárias de um grupo de empresas, independentemente do seu país de implantação, bem como por todos os

empregados de uma mesma entidade jurídica ou de um mesmo grupo de empresas. Existem dois tipos de RVE: (i) os RVE

«responsáveis pelo tratamento» que permitem enquadrar as transferências efetuadas no âmbito de um grupo agindo na qualidade de responsável pelo tratamento, e (ii) os RVE «subcontratantes» que permitem criar uma esfera de segurança para as transferências efetuadas quando o grupo age na qualidade de subcontratante;

«Avaliação de impacto sobre a proteção de dados» ou **«Data Protection Impact Assessment»** ou **«AIPD»** significa que o responsável pelo tratamento efetua, antes de qualquer tratamento suscetível de criar um risco elevado para os direitos e as liberdades das pessoas singulares, nomeadamente, através da utilização de novas tecnologias, uma análise do impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Uma única e mesma análise pode incidir num conjunto de operações de tratamento semelhantes que apresentam riscos elevados semelhantes.

Índice

1. Contexto

Na qualidade de prestador de serviços de restauração, a segurança alimentar constitui um aspeto fundamental da atividade do Grupo Elior. Propor uma alimentação saudável, preparada e distribuída em conformidade com a regulamentação em vigor aos seus clientes e convivas é uma preocupação constante do Grupo Elior e constitui um dos fundamentos da confiança que lhe depositam. Neste mesmo regime, a realização de tratamentos de dados pessoais em conformidade com a legislação em vigor constitui um desafio fundamental para o Grupo Elior.

Com efeito, a rápida evolução das tecnologias e a globalização conduziram a um aumento substancial dos fluxos de intercâmbio de dados pessoais entre intervenientes, o que se traduz em novos desafios para a proteção dos DP. O volume da recolha e da partilha de dados pessoais aumentou significativamente, o que favorece a sua utilização e a valorização destes dados sem precedentes. O Grupo Elior, com a ambição de se distinguir pela inovação tecnológica no domínio digital e pela capacidade crescente de recolher e explorar dados, inscreve-se plenamente nesta tendência. Os dados são omnipresentes e, de hoje em diante, posicionam-se no centro da cadeia de criação de valor. Bem geridos e seguros, permitem ganhar em eficácia e competitividade, personalizar e reforçar a relação com os clientes e os convivas, conquistar novos mercados, melhorar os produtos e serviços e facilitar a colaboração e a mobilidade.

Isto não pode ser feito sem o estabelecimento da confiança que permitirá o desenvolvimento do posicionamento digital do Grupo Elior, garantindo às equipas, aos clientes, aos convivas e, de uma forma mais geral, a todos os interlocutores do Grupo Elior o controlo dos dados pessoais que lhes digam respeito.

Perante a emergência de quadros legislativos nacionais e supranacionais, o Grupo Elior procura constantemente adaptar-se aos desafios do setor digital e construir uma abordagem de melhoria contínua e de conformidade da gestão de dados pessoais.

2. Âmbito

O Grupo Elior trabalha constantemente com dados pessoais no âmbito das suas atividades, por exemplo:

- na captação de imagens com a ajuda de câmaras de videovigilância;
- no tratamento de pedidos apresentados pelos clientes;
- na recolha de regimes alimentares dos convivas para lhes serem servidas refeições adequadas;
- ou ainda, na recolha de informações sobre as equipas no âmbito da gestão das suas carreiras.

A presente política é aplicável a todos os colaboradores, colaboradoras, parceiros e subcontratantes do Grupo Elior sempre que sejam recolhidos, utilizados, tornados acessíveis ou partilhados dados pessoais relativos a clientes, convivas, equipas, fornecedores ou outras pessoas singulares.

Tendo em conta a localização da sede social do Grupo Elior em França, esta política visa, nomeadamente, responder às obrigações estabelecidas pelo Regulamento (UE) 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 destes dados, adiante designado o «Regulamento Geral sobre a Proteção de Dados», o «Regulamento» ou o «RGPD».

Esta abordagem inscreve-se na vontade de harmonizar superficialmente as práticas no Grupo Elior, de simplificar o acompanhamento e a manutenção, ao longo do tempo, da conformidade e de garantir um elevado nível de proteção de dados pessoais. Para alcançar este objetivo, a presente política deve ter em conta, na medida do possível, as especificidades nacionais:

- dentro do Espaço Económico Europeu, em paralelo com o Regulamento Geral sobre a Proteção de Dados, pelo cumprimento das disposições legislativas nacionais específicas que estipulem as condições em que o tratamento de dados pessoais é lícito;
- fora do Espaço Económico Europeu, tomando em consideração, em todos os Estados onde o Grupo Elior esteja presente, uma legislação nacional específica da proteção de dados pessoais, ou mesmo uma autoridade especificamente competente para a sua aplicação.

Convém esclarecer que o direito à proteção de dados pessoais não é um direito absoluto, deve ser considerado em relação à sua função na sociedade e ser contrabalançado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade, nomeadamente, o respeito pela vida privada e familiar, pelo domicílio e das comunicações, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação ou ainda da liberdade de empreendimento. Esta política não visa definir o equilíbrio entre estes direitos, que deverá ser analisado caso a caso pelos serviços jurídicos do Grupo Elior, tendo em conta a evolução da jurisprudência e as recomendações das autoridades.

3. Governação

A. Quadro geral

A abordagem de controlo da gestão de dados é gerida por uma **equipa do Grupo** composta por:

- Um **Diretor responsável pela conformidade do Grupo**: diretamente subordinado ao diretor-geral, é responsável pela aplicação das regras de conformidade. É o garante da tomada em consideração a um nível ideal da proteção de dados pessoais no Grupo Elior;

- Um **Responsável pela proteção de dados do Grupo** (RPD): é o garante da aplicação do programa de proteção de dados pessoais e do cumprimento da legislação associada para todo o Grupo Elior. Possui um bom conhecimento das técnicas e da organização do Grupo Elior, nomeadamente, das operações de tratamento, dos sistemas de informação e das necessidades do Grupo Elior em matéria de proteção e de segurança de dados. Exerce as suas funções e missões com total independência e pode contar com o apoio do **Diretor de conformidade em matéria de segurança de TI do Grupo**.

- Um **Consultor jurídico sénior do Grupo**: acompanha e aconselha o RPD na compreensão e na interpretação dos textos jurídicos e na relação com as autoridades de proteção de dados pessoais. É também o garante da tomada em consideração das problemáticas de proteção de dados pessoais no âmbito das relações contratuais.

A equipa do Grupo apoia-se em intervenientes descentralizados no Grupo Elior: os **embaixadores dos DP**. Estes embaixadores dos DP são os pontos de contacto do RPD no seu âmbito e contribuem, nomeadamente, para:

- a construção das políticas e os procedimentos associados;
- a garantia da conformidade com a política do Grupo, nomeadamente, no que respeita ao exercício dos direitos e à manutenção do registo dos tratamentos;
- ser os pontos de contacto privilegiados no que respeita à equipa do RGPD do Grupo e do seu âmbito para qualquer questão relativa aos DP.

A presente política é revista anualmente, por iniciativa da equipa do RGPD do Grupo, para ter em conta qualquer evolução da legislação ou das práticas internas no Grupo Elior. Faz parte da liberdade de cada uma das filiais do Grupo Elior organizar-se internamente e definir a presente política para facilitar a sua difusão e aplicação.

B. Ferramenta de conformidade

O Grupo Elior dotou-se recentemente de um programa de gestão da conformidade, que permite responder às obrigações relativas à proteção de dados pessoais e gerir as diligências associadas ou ainda acompanhar as suas equipas no cumprimento das regras de conformidade no âmbito das suas atividades.

Todos os colaboradores do Grupo Elior, chamados a assumir responsabilidades no tratamento de dados pessoais (ou seja, os responsáveis pelo sistema de informação e técnicos, bem como os embaixadores dos DP) têm acesso a este ambiente. Esta ferramenta permite, nomeadamente:

- manter os registos de tratamento atualizados (responsável pelo tratamento/subcontratantes);
- acompanhar os responsáveis de projeto na aplicação das exigências relativas à proteção de dados;
- gerar formulários de contacto para o exercício dos direitos das pessoas e gerir o seu tratamento;
- manter um registo dos subcontratantes;
- gerir as notificações de incidentes;
- de uma forma mais geral, permitir o cumprimento da legislação no Grupo Elior em conformidade com o princípio da responsabilização.

No entanto, é da responsabilidade:

- dos gestores de projeto (responsáveis pelo sistema de informação e técnicos) que informem qualquer novo tratamento de dados dentro deste ambiente e os embaixadores dos DP que acompanhem e validem as informações fornecidas;
- dos embaixadores dos DP que garantam o correto tratamento dos pedidos de exercício dos direitos com o apoio dos responsáveis pelo sistema de informação e técnicos.

C. Comité diretivo para os DP (CD DP)

Dinamizado pelo RPD e sob a presidência do Diretor responsável pela conformidade do Grupo, o comité diretivo dos dados pessoais é a instância decisória.

Assume, nomeadamente, as seguintes atribuições relativas à proteção de dados pessoais no Grupo Elior:

- validar a política e as suas evoluções;
- elaborar o balanço anual das ações;
- registar o nível de conformidade;
- validar e arbitrar a prioridade das ações.

Em complemento à equipa do Grupo, o CD DP é composto pelos seguintes membros:

- o diretor dos sistemas de informação do Grupo;
- o diretor jurídico do Grupo;
- o diretor de auditorias internas do Grupo;
- o diretor responsável pelos seguros e prevenção de riscos do Grupo;
- os diretores dos sistemas de informação das operações;
- os diretores jurídicos das operações.

A recolha das decisões do CD DP será formalizada pelo RPD no final dos comités. Os relatórios estarão acessíveis a todas as partes interessadas.

O CD DP reúne-se anualmente. Pode reunir-se extraordinariamente por ocasião de um evento considerado significativo, sob proposta do RPD (incidente maior, arbitragem importante, controlo das autoridades, etc.).

D. Grupo de trabalho relativo à proteção de dados pessoais (GT)

Dinamizado pelo Diretor de conformidade em matéria de segurança de TI e o Consultor jurídico sénior do Grupo sob a presidência do RPD, o Comité operacional para os DP é a instância de planificação e acompanhamento das recomendações emitidas pelo CD DP.

Em complemento à equipa do Grupo, estão também presentes os embaixadores dos DP das áreas (restauração coletiva, restauração de concessões e serviços) e, conforme apropriado, os embaixadores dos DP a nível internacional.

O CD DP reúne-se quando é oportuno.

E. Dinamização transversal

O Diretor de conformidade em matéria de segurança de TI é responsável pela dinamização dos trabalhos relativos à proteção de dados pessoais em França e a nível internacional. Tem também por missão identificar e divulgar as boas práticas associadas no Grupo Elior.

4. As nossas obrigações

A presente secção descreve as várias obrigações relacionadas com a proteção de dados pessoais que competem ao Grupo Elior.

A. Responsabilidade e inventários dos tratamentos

O Regulamento Geral sobre a Proteção de Dados introduz o princípio de responsabilização, ou *accountability*, no âmbito do tratamento de dados. Desde a sua entrada em vigor, o Grupo Elior deve ser capaz de demonstrar a sua conformidade com o regulamento, o que passa, nomeadamente, pela realização da aplicação do inventário dos tratamentos de dados.

Sendo assim, há dois tipos de registos a manter no Grupo Elior: o primeiro diz respeito aos tratamentos para os quais qualquer entidade do Grupo Elior é responsável pelo tratamento e o segundo diz respeito aos tratamentos para os quais qualquer entidade do Grupo Elior age na qualidade de subcontratante.

Para cada um dos tratamentos em que o Grupo Elior age como responsável pelo tratamento, as seguintes informações devem constar do registo:

- a identidade do responsável pelo tratamento e dos subcontratantes;
- a identidade e os dados de contacto dos responsáveis pelo sistema de informação e técnicos;
- a finalidade (o objetivo pretendido pela recolha e o tratamento de dados);
- a base jurídica para o tratamento;
- a lista dos dados recolhidos, o seu prazo de conservação e os titulares dos dados;
- as categorias de pessoas com acesso aos dados (administrador, recursos humanos, subcontratantes, etc.);
- a presença de transferências para um país terceiro;

- a forma como a informação das pessoas é realizada;
- as medidas de segurança aplicadas;
- eventualmente, os resultados da AIPD.

Para cada um dos tratamentos em que o Grupo Elior age como subcontratante, as seguintes informações devem constar do registo:

- o nome e os dados de contacto de cada cliente por conta do qual os dados são tratados;
- o nome e os dados de contacto de cada subcontratante subsequente, se for caso disso;
- as categorias dos tratamentos efetuados por conta de cada cliente;
- as transferências de dados para fora da UE por conta do cliente;
- na medida do possível, uma descrição geral das medidas técnicas e organizacionais de segurança aplicadas.

Compete aos responsáveis pelo sistema de informação e técnicos informarem este registo com base nos seus embaixadores dos DP.

B. Transparência e equidade

Transparência

O Grupo Elior e as suas equipas têm o dever de ser claros e transparentes no tratamento de dados pessoais. Os dados recolhidos não devem ser utilizados de uma forma e com um objetivo que não sejam razoavelmente esperados e previstos para a finalidade pretendida.

Por conseguinte, antes de recolher dados pessoais, é necessário comunicar em linguagem clara e simples sobre:

- quem somos;
- quais são os dados pessoais recolhidos e qual é a sua origem;
- as operações a realizar com estes dados pessoais e a base jurídica;
- se os dados pessoais são ou serão partilhados com outros destinatários;
- O prazo de conservação dos dados pessoais;
- se os dados pessoais serão transferidos para fora do Espaço Económico Europeu;
- os direitos garantidos às pessoas relativos ao tratamento de dados pessoais.

Legalidade do tratamento

Para que o tratamento de dados pessoais seja lícito, é necessário ter razões legítimas ou justificar obrigações jurídicas ou então obter o consentimento do titular dos dados. Assim, antes de qualquer tratamento de dados pessoais, em complemento da informação das pessoas, convém garantir que este se baseia numa das seguintes bases:

- **Obrigação jurídica**: o tratamento é necessário para o cumprimento de uma obrigação jurídica à qual o responsável pelo tratamento está sujeito (direito nacional ou direito da União Europeia); por exemplo, a comunicação à segurança social e à administração fiscal dos dados relativos à remuneração dos empregados.

- **Necessidade contratual**: o tratamento é necessário para a execução de um contrato no qual o titular dos dados é parte outorgante ou para a execução de medidas pré-contratuais tomadas a pedido deste.
  Esta situação deve abranger apenas os serviços essenciais à realização do contrato e, nomeadamente, excluir qualquer *marketing* direto; por exemplo, a recolha dos dados de um conviva para a edição e o envio de faturas ou ainda o tratamento dos dados dos empregados para a aplicação do pagamento.

- **Interesses legítimos**: o tratamento é necessário para fins dos interesses legítimos pretendidos pelo responsável pelo tratamento ou por terceiro, desde que não prevaleçam os interesses ou os direitos e as liberdades fundamentais do titular dos dados, que exigem a proteção de dados pessoais. O interesse legítimo do responsável pelo tratamento deve, então, ser sempre equilibrado com os direitos e as liberdades fundamentais dos titulares dos dados; por exemplo, a comunicação de elementos relacionados com a corrupção a uma autoridade fora da União Europeia ou a análise do tráfego na Internet para impedir o acesso a sistemas maliciosos com vista à segurança da rede informática.

- **Interesses vitais**: o tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; por exemplo, a recolha de um número de telefone pessoal para o envio de SMS de alerta, em caso de eventos graves no local de trabalho ou a recolha de dados relativos a um regime alimentar específico para evitar qualquer risco para a saúde de uma pessoa.

- **Interesse público**: esta base jurídica diz respeito à situação em que o responsável pelo tratamento é investido por uma autoridade pública ou por uma missão de interesse público, para a qual é necessário o tratamento. No caso em que esta situação possa surgir, esta base jurídica deve ser utilizada caso a caso, após validação por um embaixador dos DP.

- **Obtenção do consentimento**: o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas:
    - O seu consentimento deve ser livre (escolha real, sem consequências negativas), específico (consentimento específico para cada finalidade), esclarecido (presença, no momento da expressão do consentimento, de informações adequadas e suficientes) e unívoco (lógica de «opt-in» ou opção de inclusão, nenhuma ambiguidade e ausência de consentimento por omissão ou associado a uma inação);
    - a obtenção do consentimento deve poder ser demonstrável, (ex.: casas a assinalar, formulário a preencher, procedimentos ou mecanismos sistemáticos) e dar à pessoa a possibilidade de o retirar.

Minimização dos dados

Além disso, as informações recolhidas e registadas devem ser pertinentes e estritamente necessárias para o objetivo pretendido. Sendo assim, devem ser tomadas medidas para reduzir, no mínimo, o volume de dados pessoais recolhidos e assegurar que estes são adequados à realização das finalidades do tratamento.

C. Manter os dados exatos e conservá-los durante um período de tempo limitado

Dispor de informações incorretas ou inexatas sobre uma pessoa pode dar origem a prejuízos. Por exemplo, uma pessoa poderia ser assim excluída das vantagens ou dos benefícios associados ao seu estatuto. Por conseguinte, devemos estar particularmente atentos quando uma decisão é tomada com base em dados pessoais.

Exatidão dos dados

Os colaboradores do Grupo Elior devem garantir que as informações de que dispõem são exatas, o que é, nomeadamente, garantido pela aplicação dos seguintes mecanismos:

- verificar a exatidão da informação no momento da recolha, sempre que possível;
- na medida do possível, dar a possibilidade aos titulares dos dados de atualizar os dados que lhes digam respeito;
- examinar periodicamente os dados pessoais conservados para garantir que continuam atualizados;
- corrigir ou eliminar os dados inexatos.

Riscos inerentes às áreas de comentários livres (ACL)

Os campos de texto e as áreas de comentários devem ser objeto de precauções especiais. Estes campos de texto livre são úteis para assegurar o acompanhamento de um caso ou para personalizar uma relação. Se não for proibido recorrer a estes campos, as ações de sensibilização e as regras de gestão devem enquadrar a sua utilização para evitar que os comentários introduzidos possam violar os direitos dos titulares dos dados.

Determinados comentários podem ser depreciativos, discriminatórios ou mesmo injuriosos, ou podem revelar dados ditos sensíveis, como os dados relativos à saúde. Os comentários devem, portanto, ser adequados, objetivos e respeitadores.

A melhor das precauções é ter em conta que os titulares dos dados (clientes, convivas, empregados, etc.) podem, a qualquer momento e, mediante simples pedido, ter acesso ao conteúdo destas áreas de comentários exercendo o seu direito de acesso.

Prazo de conservação

Os dados pessoais não podem ser conservados indefinidamente, pelo que um prazo de conservação deve ser determinado em função do objetivo que levou à recolha destes dados. Uma vez atingido este objetivo, estes dados devem ser, consoante o caso, arquivados, eliminados ou anonimizados (nomeadamente, para fins de produção de estatísticas).

É importante notar que, no interesse legítimo do Grupo Elior e na defesa dos seus interesses, estes dados poderão, no entanto, ser conservados por prazos mais longos, justificados por um contexto específico, no âmbito do contencioso, por exemplo, e em todos os casos após notificação ao RPD.

D. Garantir a segurança dos dados

A segurança dos dados é uma questão importante para o Grupo Elior. O facto de não se garantir a segurança dos dados no conjunto do seu ciclo de vida, desde a sua recolha até à sua destruição, pode acarretar prejuízos significativos para as pessoas. Deve ser prestada atenção acrescida à segurança dos prestadores de serviços externos quando estes são partes interessadas no tratamento de dados pessoais.

Existem muitas formas de proteger os dados pessoais, sejam estes conservados em formato eletrónico ou em papel. Para acompanhar as suas equipas, o Grupo Elior mantém à sua disposição um grupo de documentos em conformidade com o estado da arte, cuja aplicação é obrigatória:

- uma política de segurança dos sistemas de informação e das diretivas associadas que descrevem as exigências aplicáveis aos sistemas de informação do Grupo Elior;
- as exigências de segurança que constituem pré-requisitos para qualquer contrato com um prestador de serviços informáticos.

As recomendações apresentadas a seguir devem ser adaptadas caso a caso e em função dos riscos induzidos pelo tratamento de dados sobre as liberdades e a privacidade dos titulares dos dados:

- as aplicações devem ser protegidas por sistemas de autenticação (nome de utilizador e palavra-passe), em conformidade com a política de segurança da informação;
- o acesso aos dados pessoais só é permitido às pessoas autorizadas a ter acesso aos dados em questão, ou seja, o «direito de conhecer»;
- seja qual for o tipo de suporte físico, digital ou em formato de papel, estes devem ser seguros. Convém estar particularmente atento no que respeita aos equipamentos móveis e não deixar sem vigilância ou proteção estes equipamentos.

Para quaisquer dúvidas, pode consultar o Responsável pela segurança dos sistemas de informação do Grupo Elior.

E. Subcontratação e transferência de dados pessoais

Em caso de transferência de dados pessoais, o Grupo Elior deve assegurar-se previamente de que a transferência é juridicamente possível e segura. A transferência de dados pessoais deve ser interpretada no sentido lato; pode tratar-se, por exemplo, de:

- transferências de dados entre entidades jurídicas no próprio Grupo Elior;
- uma administração ou manutenção externalizada de um recurso informático;
- um alojamento de um serviço na nuvem.

Obrigações do subcontratante

Em conformidade com o RGPD, o subcontratante deve acompanhar o responsável pelo tratamento na sua abordagem constante de conformidade. É da responsabilidade do responsável pelo tratamento garantir que o subcontratante cumpre essa missão. Deve ser esperado do subcontratante uma obrigação de:

- **transparência**: possibilitada pela redação de um ato jurídico (i) que define claramente as obrigações de cada uma das partes, (ii) que especifica que o subcontratante age apenas mediante instrução do responsável pelo tratamento. Esta transparência também é garantida pela manutenção de um registo atualizado das atividades efetuadas por conta do responsável pelo tratamento e pela disponibilização de todas as informações necessárias para demonstrar o cumprimento destas obrigações;
- **aconselhamento e assistência**: o subcontratante deve acompanhar o responsável pelo tratamento na determinação dos dados estritamente necessários, no tratamento dos pedidos de exercício dos direitos e, de uma forma mais geral, em todas as suas obrigações;
- **segurança**: o subcontratante deve garantir que os seus empregados estão sujeitos a uma obrigação de confidencialidade e deve tomar todas as medidas necessárias para garantir um nível de segurança adequado aos riscos e uma conservação de dados durante o prazo estrito previsto;
- **notificação**: o subcontratante deve notificar o responsável pelo tratamento de qualquer violação de dados dentro de um prazo razoável (idealmente 24 ou 36 horas).

O Grupo Elior e as suas equipas comprometem-se a garantir o cumprimento destas exigências para cada recurso a subcontratantes e quando o Grupo Elior age na qualidade de subcontratante.

Quando o Grupo Elior age na qualidade de responsável pelo tratamento e recorre a um ou mais subcontratantes, este(s) último(s) respeitará(ão) as exigências do Grupo Elior em matéria de proteção de dados pessoais. A transferência de dados para subcontratantes deve ser efetuada de forma segura. É da responsabilidade do Grupo Elior garantir que os seus subcontratantes aplicam medidas adequadas para garantir a segurança dos dados pessoais.

As direções jurídicas devem ser consultadas de forma sistemática para verificar se todos os contratos preveem os requisitos necessários em matéria de proteção de dados pessoais.

Casos particulares de transferências fora do Espaço Económico Europeu (EEE):

A transferência de dados pessoais para fora do EEE deve ser enquadrada por mecanismos adequados, por exemplo:

- a assinatura de cláusulas-tipo nos contratos aprovadas pela Comissão Europeia;
- a redação de regras vinculativas aplicáveis à empresa: RVE «responsável pelo tratamento» ou RVE «subcontratante»;
- a assinatura de contratos específicos (ex.: «Privacy Shield» ou Escudo de privacidade) para os organismos com sede fora do EEE.

F. Exercício dos direitos

O Grupo Elior garante que os titulares dos dados possam usufruir plenamente dos seus direitos, nomeadamente:

- obter acesso aos dados pessoais que lhes digam respeito;
- solicitar a retificação dos dados pessoais que lhes digam respeito;
- solicitar a portabilidade dos dados pessoais que lhes digam respeito em formato estruturado;
- opor-se a uma decisão baseada exclusivamente num tratamento automatizado;
- solicitar a eliminação dos dados pessoais;
- solicitar a limitação do tratamento dos dados pessoais;
- opor-se ao tratamento dos dados pessoais.

G. «Privacy by design» (Privacidade desde a conceção)

É mais simples e menos dispendioso ter em conta as considerações sobre a privacidade e a segurança o mais rapidamente possível nos projetos. É por isso que, a partir do início de um novo projeto, compete ao responsável pelo projeto ter em conta a problemática da proteção de dados pessoais e assegurar o respeito da privacidade dos titulares dos dados, seja na aplicação de um novo serviço/produto, seja no momento da sua modificação.

Isso significa, nomeadamente, que, para qualquer novo projeto, o responsável pelo projeto deve:

- identificar os dados pessoais suscetíveis de estarem presentes;
- se for caso disso:
    - informar-se sobre este projeto no âmbito da ferramenta de gestão da proteção de dados pessoais e acompanhar as indicações,
    - identificar os principais riscos ligados aos dados pessoais que podem surgir no âmbito de um determinado projeto, nomeadamente, os riscos jurídicos, os riscos associados à reputação e os riscos para as pessoas,
    - para o tratamento de dados de alto risco, realizar uma avaliação de impacto sobre a proteção de dados (AIPD). Estes tratamentos incluem, nomeadamente, a utilização de dados em grande escala, a utilização de novas tecnologias, o tratamento de dados sensíveis, o controlo sistemático ou a aplicação do tratamento com vista à tomada de decisões automatizadas e perfis. O Comité Europeu para a Proteção de Dados refere no seu sítio Web, para cada país, a lista de tratamentos para os quais a AIPD é obrigatória,
    - assegurar-se da conformidade com a política do Grupo,
    - garantir a aplicação e o controlo dos mecanismos de proteção organizacionais e técnicos.

Em caso de necessidade de acompanhamento ou de especificações, o responsável pelo projeto pode recorrer aos seus embaixadores dos DP.

H. Comunicação e sensibilização

Anualmente, em função dos desafios identificados e das constatações relativas à conformidade do Grupo Elior, é iniciado um plano de comunicação e de sensibilização pela equipa do Grupo com o apoio dos embaixadores dos DP. Esta abordagem deve ter como objetivo instaurar uma cultura da proteção de dados pessoais no Grupo Elior.

As equipas são convidadas a contribuir para a melhoria da política e dos processos associados.

I. Categorias específicas dos tratamentos e dos dados pessoais

Dados pessoais sensíveis ou assimilados

Trata-se de informações que revelam a origem racial ou étnica, as opiniões políticas, filosóficas ou religiosas, a filiação sindical, a saúde ou a vida sexual de uma pessoa singular. As informações sobre infrações ou condenações também devem ser consideradas como tal.

Recomenda-se que no Grupo Elior não se recolha nem utilize estes dados devido aos elevados riscos que envolvem a privacidade das pessoas, salvo em determinados casos específicos:

- se o titular dos dados tiver dado o seu consentimento expresso (escrito, claro e explícito);
- se estes dados forem necessários para fins médicos ou para a investigação no domínio da saúde;
- se a sua utilização for autorizada pela autoridade de proteção de dados pessoais.

Estes casos podem variar de acordo com a legislação nacional do país, pelo que convém dirigir-se aos embaixadores dos DP ou à equipa do RGPD do Grupo para este tipo de problemáticas. Deverá ser sempre realizada uma AIPD.

Dados pessoais e direito à imagem relativos às crianças

As crianças merecem uma proteção específica no que respeita aos seus dados pessoais, porque podem estar menos conscientes dos riscos, das consequências ou das garantias que devem ser dadas e dos seus direitos associados ao tratamento de dados pessoais.

No âmbito dos serviços da sociedade da informação, o tratamento dos dados pessoais relativos a uma criança é lícito quando a criança tem, pelo menos, 16 anos. Quando a criança tem menos de 16 anos, este tratamento só é lícito no caso e na medida em que o consentimento for dado ou autorizado pelo titular da responsabilidade parental sobre a criança. Os Estados-Membros podem prever por lei uma idade inferior para estas finalidades, desde que esta idade inferior não seja inferior a 13 anos. Não hesite em dirigir-se ao embaixador dos DP para identificar o limite de idade em função do tratamento previsto.

Deve ser sempre realizada uma AIPD antes da aplicação destes tratamentos.

Operações de marketing

As operações de *marketing* devem respeitar as escolhas e os direitos dos titulares dos dados. Durante as operações de *marketing*, nomeadamente, por via eletrónica, é conveniente assegurar-se de que:

- os titulares dos dados deram o seu consentimento expresso (para as relações «BtoC» ou empresa ao consumidor);
- os titulares não exerceram o seu direito de oposição à prospeção;
- as mensagens dão a possibilidade de cancelar a assinatura facilmente («opt-out» ou opção de exclusão);
- nenhum destinatário pode ver os nomes e os dados de contacto de outro destinatário.

J. Violações de dados

Apesar da aplicação de normas de alto nível para garantir a segurança dos dados, o Grupo Elior não pode precaver-se totalmente do risco de violações de dados que possam ser definidas por:

- uma violação à confidencialidade, ou seja, uma fuga de dados (ex.: perda da *pen* USB que contenha ficheiros de clientes);
- uma violação à integridade, ou seja, uma modificação não prevista (ex.: modificação não desejada da base de dados que indica automaticamente às autoridades o atributo de um veículo de função);
- uma violação à disponibilidade, ou seja, uma destruição de dados (ex.: programa malicioso que codifique uma base de dados).

A origem destas violações pode ser tanto externa (ex.: ataque a um recurso do Grupo Elior ou de um prestador de serviços exposto à internet) como interna. Pode também ser intencional ou acidental (ex.: ecrã não protegido por um filtro de confidencialidade exposto nos transportes públicos).

É da responsabilidade de cada um estar atento e notificar imediatamente qualquer violação de dados à equipa do RGPD do Grupo. Em caso de violação, comprovada ou presumível, à segurança, convém agir imediatamente para limitar os efeitos e os danos. Nos casos mais graves, o Grupo Elior deverá informar a autoridade competente de proteção de dados pessoais e fornecer-lhe um plano de ação que permita mitigar os efeitos da violação no prazo de 72 horas e, em alguns casos, informar também os titulares dos dados.

K. Controlo e relação com as autoridades de proteção de dados

Impacto potencial da não consideração da proteção de dados pessoais

As infrações à legislação sobre a proteção de dados pessoais podem ter graves consequências, nomeadamente:

- sanções financeiras até 4 % do volume total de negócios do Grupo Elior;
- pedidos de indemnização dos titulares dos dados afetados pela violação à privacidade;
- a conformidade sob obrigação, a limitação de um tratamento ou a suspensão dos fluxos de dados;
- violação à reputação e à imagem do Grupo Elior.

Poder das autoridades de proteção de dados

O Grupo Elior está em vias de elaborar as *Binding Corporate Rules* ou regras vinculativas aplicáveis à empresa. Estas RVE têm como objetivo demonstrar o cumprimento de um nível de proteção de dados semelhante, independentemente da área de localização da entidade jurídica filial do Grupo Elior e de autorizar as transferências de dados pessoais no Grupo Elior.

A autoridade de proteção de dados pessoais dispõe do poder de controlar a conformidade com o Regulamento Geral sobre a Proteção de Dados através de controlos físicos ou à distância e pode nomeadamente:

- obter cópia do máximo de informações técnicas e jurídicas, para apreciar as condições em que são aplicados os tratamentos de dados pessoais;
- solicitar a comunicação de todos os documentos necessários para o cumprimento da sua missão;
- obter acesso aos programas informáticos e aos dados e solicitar a sua transcrição;
- solicitar cópia de contratos (ex.: contratos de locação de ficheiros, contratos de subcontratação informática), formulários, processos, documentos, bases de dados, etc.
- realizar à distância análises de vulnerabilidade, auditorias de segurança e verificar a presença das menções de informação legal.

Em França, o artigo 51.º da lei n.º 78-17 de 6 de janeiro de 1978, alterada, relativa à informática, aos ficheiros e às liberdades, designada «lei informática e liberdades», dispõe que qualquer entrave à ação da CNIL (Comissão Nacional de Informática e das Liberdades) é punido com um ano de prisão e com multa de 15 000 €. O entrave à ação da autoridade de proteção de dados pessoais é realizado em caso de:

- oposição ao exercício das missões confiadas aos membros ou agentes habilitados quando a visita foi autorizada pelo «juge des libertés et de la détention» (juiz competente em matéria de liberdades e de detenção);
- recusa de comunicação, ocultação ou destruição das informações e dos documentos úteis à missão de controlo;
- de comunicação de informações não conformes ao conteúdo dos registos tal como era no momento em que o pedido da autoridade de proteção de dados pessoais foi formulado ou de apresentação de um conteúdo sob uma forma que não é diretamente acessível.

Conduta a manter:

Recomenda-se contactar imediatamente a equipa do Grupo e cooperar plenamente com as autoridades após verificação da identidade das pessoas (mandato e carteira profissional).

A equipa do Grupo é a única entidade habilitada a comunicar com as autoridades de proteção de dados (ex.: abordagem prévia, pedido de informação, resposta a consultas, etc.). Qualquer solicitação das autoridades deve, pois, ser-lhe notificada sem demora.

5. Informação complementar

Se tiver dúvidas sobre esta política ou desejar obter mais informações sobre qualquer um dos assuntos tratados, pode contactar a equipa do Grupo através do seguinte endereço de correio eletrónico: gdpr-contact@eliorgroup.com.