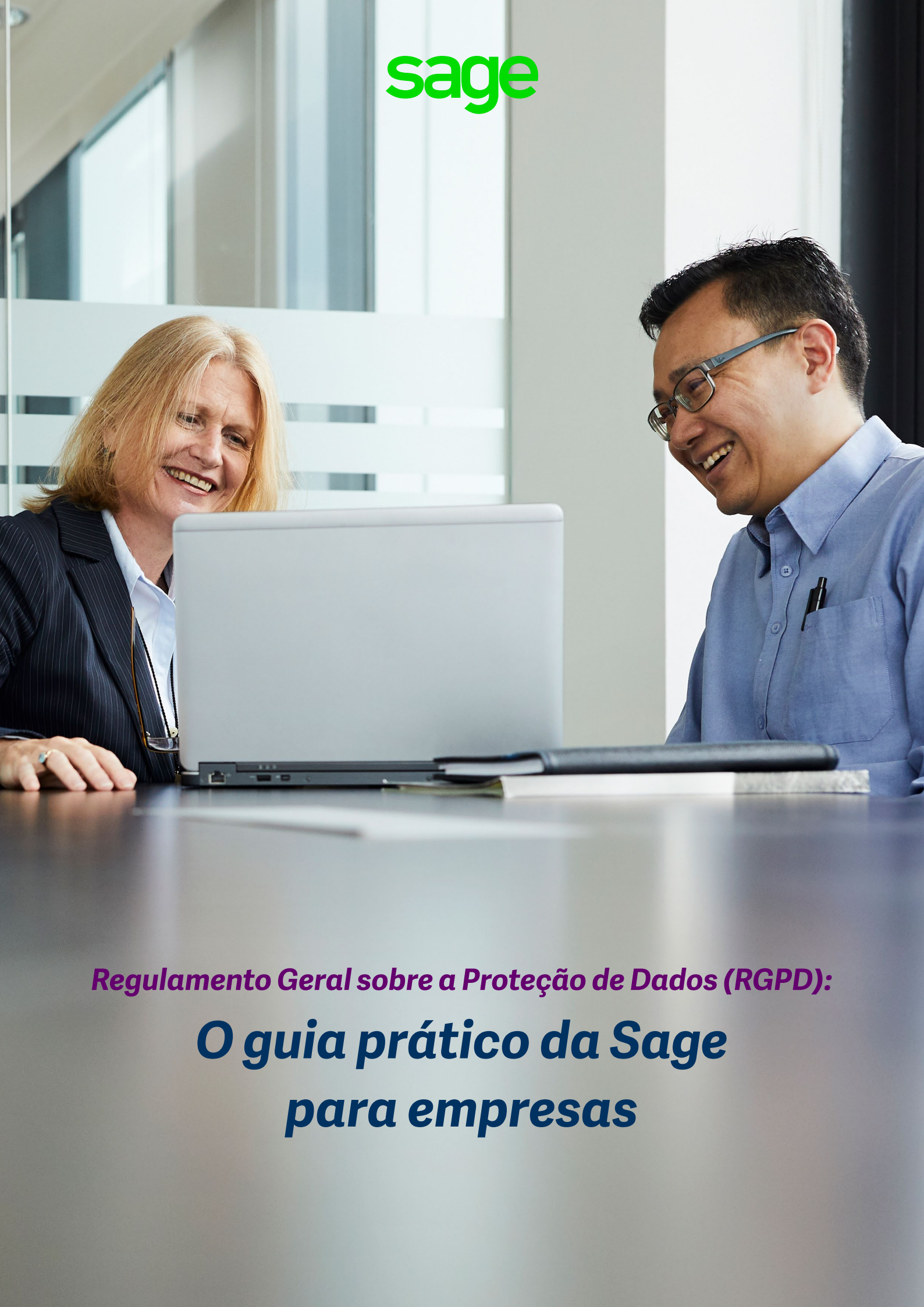


Regulamento Geral sobre a Proteção de Dados (RGPD):

O guia prático da Sage para empresas

Conteúdo

Introdução 3

Infográfico: Visão geral do RGPD 4

O essencial 5

Resumindo o RGPD

- Direitos individuais—e como informar as pessoas sobre eles 5
- Consentimento 5
- Direito de mover ou transferir dados pessoais (portabilidade de dados) 6
- Um âmbito de aplicação bem maior 6
- Prova de conformidade 6
- Privacidade do início ao fim 6
- Comunicação obrigatória de infrações 7
- Responsável pela proteção de dados (RPD) 7
- Penalidades 7

Brexit 7

Princípios básicos do RGPD 8

- Princípios da proteção de dados 8
- Licitude do tratamento 8
- Transferências internacionais 8

Ações que você pode tomar agora 8

Isenção de responsabilidade legal da Sage 9

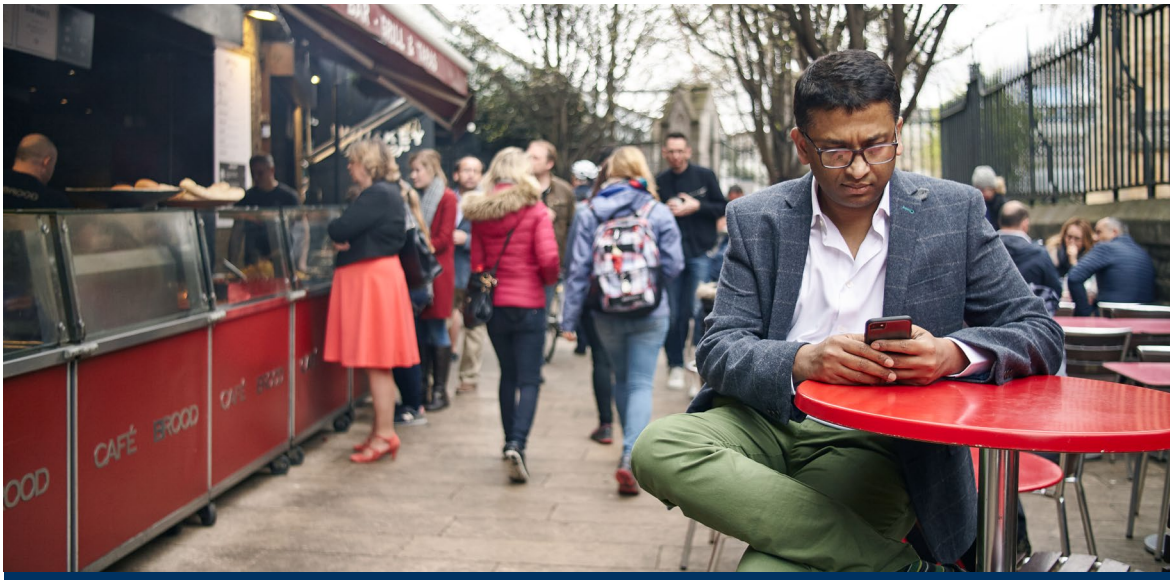
Introdução

O Regulamento Geral sobre a Proteção de Dados ("RGPD") é a nova estrutura jurídica que entrará em vigor a partir de 25 de maio de 2018 na União Europeia ("UE"). Os regulamentos da UE têm efeito direto em todos os estados-membros da UE, o que significa que o RGPD terá precedência sobre quaisquer leis nacionais.

O foco do RGPD é a proteção dos dados pessoais, ou seja, dados referentes a pessoas. Na verdade, o RGPD é uma das maiores mudanças já vistas que afetam como os dados relacionados a um indivíduo devem ser tratados e, potencialmente, afeta não apenas as empresas, mas também qualquer indivíduo, corporação, autoridade pública, agência ou outra estrutura que processe os dados pessoais de pessoas que estão baseadas na UE. Isso inclui provedores e outros terceiros que uma empresa possa utilizar para o processamento de dados pessoais.

Ele tem um escopo bem abrangente e inclui todos os estados-membros da União Europeia, além do Reino Unido pós-Brexit em 2019, pois o RGPD será incorporado à legislação do Reino Unido. Diferentemente das regras de proteção de dados da Diretiva 95/46 da UE, o RGPD também afeta quaisquer empresas fora da UE que ofereçam produtos ou serviços a pessoas na UE ou que monitorem o comportamento delas dentro da UE. Por exemplo, empresas de hospedagem de sites nos EUA que hospedam sites que podem ser acessados por pessoas na UE serão diretamente afetados.

O RGPD tem implicações imensas para todos os departamentos de muitas empresas no mundo todo. Algumas podem precisar contratar ou designar um Responsável pela Proteção de Dados, por exemplo. Praticamente todas deverão implementar práticas e salvaguardas adicionais. É muito recomendado realizar uma auditoria por alguém com qualificação apropriada e com a possibilidade de incorrer em multas de até 4% do volume de negócios anual global ou de 20 milhões de euros, o que for maior, o conhecimento do RGPD deve ser considerado obrigatório.



Este documento consiste num guia conciso e simplificado para empresas. Mais informações podem ser obtidas com as autoridades supervisoras, como o site da Comissão Nacional de Proteção de Dados (ICO) no Reino Unido e sua "Visão geral do Regulamento Geral sobre a Proteção de Dados". Leia a Declaração de isenção de responsabilidade da Sage, no final deste guia.

Infográfico:

Visão geral do RGPD

Regulamento Geral sobre a Proteção de Dados (RGPD)

Consentimento

Deve ser confirmado com uma declaração ou outra clara ação afirmativa. O consentimento não deve ser presumido, nem devem ser usados campos pré-marcados.

Encarregado da proteção de dados

Deve ser obrigatório. Requer conhecimento especializado da lei de proteção de dados. Pode ser um funcionário ou contratado para a função.

Privacidade do princípio ao fim

As considerações de privacidade devem ser incorporadas em toda parte e apenas os dados estritamente necessários para o fim especificado podem ser usados.

Âmbito muito mais amplo

Abrange sua empresa e aqueles que processam dados para você - mesmo fora da UE.

Comunicação obrigatória de infrações

Os responsáveis pelo controle dos dados devem informar às autoridades supervisoras, como o ICO no Reino Unido, em até 72 horas após terem tomado conhecimento. Em caso de infrações sérias, os indivíduos devem ser comunicados.

Portabilidade de dados

Os indivíduos têm agora o direito de mover, copiar ou transferir os seus dados pessoais, até para uma empresa concorrente.

Penalidades

Podem chegar a 4% do volume mundial de negócios das empresas ou a 20 milhões de euros, o que for maior. Você poderá ser multado, mesmo se não houver uma perda real dos dados.

Direitos individuais

Amplia muito os direitos dos indivíduos e quais informações devem ser fornecidas em relação às atividades de processamento.

O essencial

O RGPD estabelece os requisitos mínimos para o tratamento de todos os dados pessoais. Dados pessoais podem ser definidos como quaisquer dados que identifiquem ou sejam relacionados a um indivíduo de diversas maneiras (incluindo coisas como aparência física ou mesmo dados biométricos).

A maioria das empresas coletam dados pessoais a partir do instante em que interagem com um indivíduo e, em alguns casos, podem nem estar cientes de que estão fazendo isso. Por exemplo, a coleta de dados pessoais pode ser tão simples quanto cookies de rastreamento de sites que identificam um usuário do seu site. Ela pode incluir até algo tão detalhado quanto o registro de um indivíduo em um banco de dados de Gestão de Relação com o Cliente ("CRM") e muito mais. Ainda que os dados pessoais possam ser coletados ou processados para o benefício exclusivo do indivíduo, isto ainda está dentro do âmbito do RGPD.

Assim como a legislação da Diretiva 95/46, o RGPD redefine três conjuntos básicos de regras relacionadas aos dados pessoais: princípios da proteção de dados, licitude do tratamento e restrições de transferências internacionais. A maioria das empresas já deve estar ciente destes pontos, assim como muitos indivíduos. Estes três conjuntos de regras são descritos com mais detalhes neste documento, e sua leitura é recomendada, mesmo que apenas para relembrar o conhecimento existente.

Entretanto, o RGPD introduz diversos novos requisitos.

Resumindo o RGPD

Aqui estão as principais áreas do RGPD, com referência particular à diretiva de proteção de dados da Diretiva 95/46 da UE.

Direitos individuais—e como informar as pessoas sobre eles

A legislação atual de proteção de dados da UE (Diretiva 95/46) dá às pessoas direitos sobre seus dados pessoais e descreve quais as informações que as empresas devem fornecer aos indivíduos, incluindo informações sobre o que aquela empresa pode fazer com aqueles dados pessoais. Com frequência isso é feito por meio de declarações de privacidade ou notificações exibidas em um site.

O RGPD amplia muito este ponto, fornecendo direitos adicionais que novamente devem ser comunicados aos indivíduos. Em particular, os indivíduos devem ser informados que têm os direitos (não exaustivos) a seguir:

1. de cumprir as exigências das autoridades supervisoras, como o ICO no Reino Unido;
2. de retirar seu consentimento do processamento de seus dados pessoais (ver abaixo);
3. de acessar seus dados pessoais e que estes sejam corrigidos ou apagados (o "direito de ser esquecido") pela empresa e também por terceiros que os tenham acessado;
4. de ser informado da existência de qualquer processamento automatizado de dados (incluindo a definição de perfis);
5. de objeção a determinados tipos de processamento, por exemplo, marketing direto e decisões baseadas unicamente em processamento automatizado;
6. de ser informado por quanto tempo os dados serão armazenados;
7. de receber os dados de qualquer Responsável pela Proteção de Dados que seja indicado;

Além disso, os indivíduos têm o direito de pedir a organizações sem fins lucrativos que exerçam direitos e façam reivindicações em seu nome, de modo similar a uma ação coletiva dos EUA.

Consentimento

Se você coleta dados com base no consentimento de indivíduos, mesmo que a legislação de proteção de dados da UE sempre tenha exigido que tal consentimento seja dado espontaneamente, seja específico e informado, com o RGPD isso deve ser confirmado por uma declaração ou outra clara ação afirmativa. Em outras palavras, caixas de consentimento pré-marcadas em sites, ou o silêncio/inatividade por parte do indivíduo após revisar uma declaração de privacidade, não constituem consentimento.

Além disso, o consentimento não pode ser estendido automaticamente, pois uma empresa não pode usar o consentimento específico de um indivíduo em uma etapa da transação como consentimento para outros tipos de processamento de dados pessoais. Consentimentos separados são necessários para diferentes operações de processamento de dados pessoais.

Por fim, os indivíduos devem não apenas ser informados de que têm o direito de retirar seu consentimento a qualquer momento, como também deve ser tão fácil para eles retirar seu consentimento quanto dá-lo.

Consentimentos existentes dados por indivíduos devem ser revistos para certificar que atendem aos requisitos do RGPD. Se houver conflitos ou ambiguidades, as empresas deverão ou estabelecer uma nova base legal para o processamento dos dados (por exemplo é necessário para o cumprimento de um contrato), obter um novo consentimento ou parar de processar aqueles dados pessoais.

Direito de mover ou transferir dados pessoais (portabilidade de dados)

As pessoas agora têm o direito de mover, copiar ou transferir seus dados pessoais de um lugar a outro, até para um concorrente. Por exemplo, uma lista de reprodução pode ser gerada para um usuário por um serviço de música e, caso esse usuário mude para um novo provedor, ele pode levar essa lista de reprodução consigo. Dessa forma, os dados pessoais devem estar em um formato estruturado, comumente utilizado e legível eletronicamente, para que possa ser facilmente utilizado e compartilhado.

O requisito para tornar os dados realmente portáteis e de fácil utilização por outros deve incorrer em ajustes significativos de Ti e, consequentemente, em custos.

Um âmbito de aplicação bem maior

Em resumo, o RGPD torna responsáveis por possíveis infrações não apenas as empresas que coletam os dados pessoais, mas também qualquer terceiro que processa os dados pessoais em nome daquela empresa, seja ele outra empresa, organização ou indivíduo. Entretanto, isto não significa que uma empresa pode simplesmente entregar os dados pessoais a um terceiro e fazer vista grossa. A empresa deve garantir que o fornecedor terceiro também está em conformidade com o RGPD.

Além disso, o potencial âmbito geográfico se estende além da UE para qualquer empresa - ou novamente, para qualquer terceiro que processe dados pessoais em seu nome - que ofereça produtos ou serviços a indivíduos na UE, ou que monitore o comportamento de indivíduos na UE. Particularmente, não importa se é ou não exigido pagamento pelos produtos ou serviços, portanto as entidades beneficentes e organizações não governamentais são incluídas no RGPD.

Como a UE é um parceiro comercial da maioria dos países, o escopo amplo do RGPD significa que ele tem implicações para muitas empresas em todo o mundo, e exigirá que elas estejam em conformidade se desejarem operar nos estados-membros da UE, seja diretamente ou como terceiros para outras empresas.

Prova de conformidade

Não é suficiente apenas cumprir o RGPD. Uma empresa deve provar que o está fazendo, conforme os requisitos de "responsabilidade" do RGPD e isto significa cumprir alguns requisitos onerosos de manutenção de registros. Em particular, devem ser mantidos os registros que detalhem atividades* de processamento, solicitações de acesso do sujeito, infrações, como são obtidos os consentimentos e Avaliações de Impacto da Privacidade (veja abaixo).

Novamente, este requisito também afeta aqueles terceiros que processam dados pessoais em nome de uma empresa, apesar dos requisitos não serem tão detalhados.

**Aplicável a empresas com mais de 250 funcionários ou empresas com menos funcionários e nas quais o processamento feito pode resultar em risco para os direitos e liberdade dos indivíduos, em que não seja ocasional, ou que inclua Categorias Especiais de Dados, como informações sobre saúde, religião ou orientação sexual.*

Privacidade do início ao fim

Medidas técnicas e organizacionais devem ser postas em prática durante toda a vida útil dos dados pessoais para atender às expectativas de privacidade do indivíduo - desde a origem até a execução e finalmente, a cessação da atividade. Isto é denominado "Privacidade desde a concepção", e significa que as considerações de privacidade devem ser incorporadas em todos os aspectos daquele processamento por padrão.

Além disso, apenas os dados pessoais estritamente necessários para aquele propósito devem ser realmente processados - o que é chamado de minimização dos dados ou "Privacidade por padrão".

Na verdade, a implementação da Privacidade desde a concepção e da Privacidade por padrão envolverá treinamento contínuo, realização de auditorias periódicas, minimização dos dados coletados, restrição de acesso aos dados pessoais conforme a "necessidade de conhecimento" e a implementação de medidas de segurança técnicas e organizacionais apropriadas, como a criação de pseudônimos e criptografia.

Comunicação obrigatória de infrações

No caso de uma infração do RGPD, as empresas que coletam dados pessoais devem informar às autoridades supervisoras - como o ICO no Reino Unido - dentro de 72 horas após terem tomado conhecimento. Os terceiros que processam os dados pessoais em nome das empresas devem informar aquelas empresas sem demora.

Se a infração implicar em um grande risco aos indivíduos relacionados, as empresas também devem notificar os indivíduos afetados sem demora.

Responsável pela proteção de dados (RPD)

Sob o RGPD, as empresas e quaisquer terceiros que processam dados pessoais em seu nome deverão nomear um Responsável pela proteção de dados (RPD) se: (i) forem uma entidade pública; (ii) se as atividades principais da empresa ou dos terceiros envolver o monitoramento de indivíduos em grande escala; ou se as atividades principais consistirem do processamento em grande escala de categorias especiais de dados pessoais, incluindo dados relacionados a condenações e infrações penais. O RPD deve ter conhecimento especializado da legislação de proteção de dados, mas não necessariamente precisa ser um funcionário; ele pode ser contratado para desempenhar a função. Os dados do RPD deverão ser comunicados às autoridades supervisoras, como o ICO no Reino Unido.

Penalidades

As penalidades para o não cumprimento do RGPD são severas e podem chegar a 4% do volume mundial de negócios das empresas ou a 20 milhões de euros, o que for maior. Você poderá ser multado, mesmo se não houver uma perda real dos dados. Deve-se notar que não há exclusões ou exceções para as pequenas empresas. Além disso, os indivíduos podem iniciar uma ação judicial coletiva, solicitando uma investigação regulatória formal se a empresa não cumprir o RGPD.

Brexit

Após as eleições gerais do Reino Unido em 2017, o governo Conservador foi reeleito por mais cinco anos. Durante este mandato, especificamente em 2019, o Reino Unido vai deixar a União Europeia. Como em todos os estados-membros da UE, o RGPD se aplicará ao Reino Unido até aquela data. Entretanto, no anúncio da nova legislação após a eleição, foi declarado que as novas leis de proteção de dados farão o seguinte:

> *"... implementar o Regulamento Geral sobre a Proteção de Dados e a nova Diretiva relativa ao tratamento de dados pelas autoridades policiais e judiciárias, cumprindo as nossas obrigações enquanto formos um estado-membro da UE e ajudar a colocar o Reino Unido na melhor posição para mantermos a nossa capacidade de partilhar dados com outros estados-membros da UE e a nível internacional depois de abandonarmos a UE."*
>
> *Fonte: Discurso da Rainha, junho de 2017*

Portanto é possível, mas não pode ser presumido, que o Reino Unido pós-Brexit venha a ser considerado pela União Europeia um país capaz de garantir proteção "adequada", podendo não ser afetado por possíveis dificuldades, como proibição de transferência de dados no âmbito da proteção de dados. Acompanhe este espaço para saber mais sobre futuras decisões.

A nova legislação do Reino Unido substitui a Data Protection Act 1998, a qual teve por base a Diretiva 95/46 da UE.

Princípios básicos do RGPD

Além dos novos requisitos descritos anteriormente, assim como a Diretiva 95/46 da UE, o RGPD redefine três conjuntos básicos de regras relacionadas aos dados pessoais. Em termos simples, eles podem ser descritos da seguinte forma:

- ***Princípios da proteção de dados:*** O tratamento dos dados pessoais tem de ser lícito, leal e transparente para os indivíduos a quem dizem respeito. Eles devem ser coletados para fins específicos, explícitos e legítimos e não devem ser processados de uma maneira incompatível com isto. Os dados pessoais coletados devem ser adequados, relevantes e limitados ao que é necessário. Eles devem ser precisos e atualizados e toda etapa razoável deve ser executada para garantir que os dados pessoais que forem imprecisos sejam apagados ou retificados sem demora. Os dados devem ser armazenados de forma que identifiquem o indivíduo apenas pelo tempo que for necessário, e devem ser processados de maneira que garanta a segurança apropriada—incluindo proteção contra perda, destruição ou danos, e acesso não autorizado ou ilegal.
- ***Licitude do tratamento:*** O processamento de dados pessoais somente é lícito se pelo menos um dos itens a seguir se aplicar: o indivíduo deu seu consentimento para um ou mais fins específicos; é necessário para um contrato do qual o indivíduo é uma das partes ou será em breve; uma obrigação legal deve ser cumprida (por exemplo, envio de registros de impostos de uma empresa); há uma tarefa que é de interesse público ou é executada no interesse de uma autoridade oficial; é necessário para interesses legítimos (ou os de um terceiro), exceto quando for substituído pelos interesses, direitos básicos e liberdades do indivíduo .
- ***Transferências internacionais:*** O RGPD mantém a proibição geral de envio de dados pessoais da Área Econômica Europeia para um país que não ofereça a proteção adequada. No momento da redação deste documento, os países considerados pela Comissão Europeia como países que garantem a proteção "adequada" são: empresas dos EUA que se enquadrem na autocertificação do Escudo de Privacidade EU-EUA (observação: isto não significa que os EUA são considerados um país que ofereça a proteção adequada), Andorra, Argentina, Canadá (limitado ao PIPEDA), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça e Uruguai. Onde não existir uma decisão de adequação, as transferências só podem ser feitas em casos limitados, como quando haja consentimento, quando forem usadas cláusulas contratuais padrão publicadas pela Comissão Europeia ou, no caso de transferências entre empresas, o uso de regras vinculativas aplicáveis às empresas.

Ações que você pode tomar agora

- Visite a área sobre reforma da proteção de dados do site do ICO para saber mais. Lá você encontrará diversos guias e informações gerais. Em particular, consulte a publicação do ICO, Preparando-se para o Regulamento Geral sobre a Proteção de Dados - os 12 passos a serem dados agora".
- Revise sua coleção de dados pessoais e sistemas de processamento de dados para garantir que eles estão em conformidade com o RGPD. Você pode considerar promover uma auditoria de conformidade com o RGPD, quer do ponto de vista jurídico, quer do ponto de vista tecnológico, entre outros.
- Assegure que seus funcionários e parceiros estejam cientes do RGPD e garanta o treinamento para prepará-los. Lembre-se que o RGPD o torna responsável por terceiros que processam dados pessoais para você.
- Busque aconselhamento jurídico para compreender melhor as implicações do RGPD para a sua empresa.

Para saber mais, acesse:
sage.com/RGPD

Declaração de isenção de responsabilidade da Sage

As informações contidas neste guia são apenas para fins de orientação geral. Elas não devem ser consideradas e nem foram concebidas, como aconselhamento jurídico. Gostaríamos de reforçar que não há alternativa para clientes que pesquisam por conta própria ou que procuram por consultoria legal se eles não tiverem certeza sobre as implicações do RGPD sobre seus negócios.

Mesmo que tenhamos feito todos os esforços para garantir que as informações contidas neste site são corretas e atualizadas, a Sage não garante a completude ou precisão deste conteúdo e as informações são fornecidas "como estão", sem nenhuma garantia, expressa ou implícita. A Sage não aceita qualquer responsabilidade por erros ou omissões e não será responsável por qualquer prejuízo (incluindo, entre outros, prejuízo pela perda de clientela ou lucros cessantes) emergentes de contrato, responsabilidade civil ou outro devido à utilização ou confiança depositada nesta informação, ou devido a qualquer ato ou decisões tomadas em virtude da utilização desta informação.

© 2017 The Sage Group plc ou os seus licenciantes. Sage, os logotipos da Sage, bem como os nomes de produtos e serviços da Sage mencionados aqui são marcas registradas do The Sage Group plc ou das suas afiliadas. Todas as outras marcas são propriedade dos seus respectivos proprietários.