Salvaguardas físicas de privacidade e segurança no âmbito do GDPR

O Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR) exige que as organizações de todo o mundo repensem as formas de acesso, utilização e manutenção dos dados pessoais. Este artigo descreve os cenários de risco para os dados que poderão resultar em intervenções administrativas e em penalizações financeiras ao abrigo do novo regulamento. Também explora as melhores práticas de segurança e privacidade físicas, uma vez que estas representam uma importante área da proteção de dados que é, muitas vezes, ignorada. Em conjunto, as salvaguardas físicas, de cibersegurança e administrativas podem ajudar a proteger os dados pessoais sensíveis e demonstram o compromisso de uma organização para com a privacidade dos dados.

Conclusões principais:

- Informe-se acerca das medidas de privacidade e de segurança físicas indicadas no GDPR para proteger os dados pessoais.
- Explore o conceito de nível razoável de privacidade e de proteção de dados definido pelos especialistas do setor.

A vida num mundo orientado para os dados
Como é habitual nas empresas de hoje em dia, a maioria das organizações recolhe e utiliza dados pessoais, que podem ser de funcionários, clientes, potenciais clientes e de terceiros. Normalmente, estes dados são armazenados em formato eletrónico para estarem disponíveis para consulta pela organização[1] e por terceiros. Além disso, a principal função de algumas organizações consiste em recolher e analisar volumes de dados pessoais.

Ainda que a quantidade e o tipo de dados recolhidos por cada organização possam variar, há um consenso geral de que encontrar esses dados nunca foi tão fácil. As pessoas deixam um grande rasto de informações quando criam perfis nas redes sociais, participam em comunidades online, fazem pesquisas na Internet, respondem a inquéritos e aproveitam ofertas promocionais e serviços "gratuitos", como o armazenamento de fotografias e a transmissão em fluxo contínuo de música.

A tecnologia contribui para o processo de criar perfis robustos sobre as pessoas através de avanços na inteligência artificial, de etiquetas eletrónicas, web beacons, cookies e de outras ferramentas de monitorização.

A combinação entre a tecnologia e os esforços de exploração de dados permite que as organizações criem vastas coleções de dados pessoais. Estes repositórios podem revelar informações como a idade, o estado civil, a data de nascimento, a formação académica, os hobbies, a religião, o histórico de emprego, as convicções políticas, as preferências de compras, as fontes de notícias preferidas, o salário, os antecedentes criminais e muitas outras informações.

Ainda que muitos destes dados estejam centralizados em bases de dados de empresas, existem bolhas de dados que estão frequentemente dispersas ao longo da cadeia de fornecimento em sistemas diferentes, sistemas esses que muitas vezes não dispõem de mecanismos para transmitir a futuros destinatários informações relativas à origem ou ao motivo pelos quais esses dados foram originalmente recolhidos. Nesta situação, os dados pessoais ficam expostos e podem ser utilizados para finalidades completamente diferentes da finalidade original para a qual foram obtidos.

A qualquer momento, várias pessoas numa organização podem aceder aos dados armazenados para, por exemplo, pagar a um funcionário, realizar um estudo de mercado, lançar uma campanha de marketing por e-mail ou para acompanhar a interação dos clientes. Todos os pontos de acesso a estes conjuntos de dados representam uma oportunidade para os dados pessoais serem utilizados indevidamente ou para caírem nas mãos erradas.

Factos importantes

O que é o GDPR?
O Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR) visa a proteção da privacidade dos indivíduos da União Europeia (UE).

Quando é que entra em vigor?
25 de maio de 2018

Quem será afetado?
Todas as empresas, independentemente da sua localização, que controlam ou processam dados pessoais de titulares de dados da União Europeia.

O que são dados pessoais?
Todas as informações relativas a uma pessoa singular ou titular de dados. Pode incluir todo o tipo de dados, tais como um nome, uma fotografia, um endereço de e-mail, informações bancárias, publicações em Web sites de redes sociais, informações médicas ou o endereço IP de um computador.

Qual é o impacto?
Uma coima de 20 milhões de euros ou de até 4% do volume de negócios anual a nível mundial (conforme o que for mais elevado). Esta é a coima máxima que pode ser aplicada às infrações mais graves.

Onde posso obter mais informações?

- Uma descrição geral do regulamento
- Leitura do regulamento
- Soluções de segurança física

65%
dos inquiridos afirmaram que os incidentes de violação de dados levaram à perda de confiança na organização em que ocorreram.[5]

Para compreender os riscos de segurança física que as organizações correm, considere estes cenários:

Um funcionário está a analisar dados sensíveis no telemóvel enquanto está no aeroporto e não repara que está alguém perto de si a olhar para o ecrã.

- Um funcionário perde o portátil e as informações armazenadas no disco rígido não estão encriptadas.
- Um funcionário afasta-se da secretária para ir buscar mais café, deixando os dados de contacto dos clientes visíveis no monitor ou na secretária, enquanto um indivíduo não autorizado passa por perto.
- Um funcionário descontente tira fotografias a documentos deixados numa impressora, a informações visíveis num ecrã e a credenciais de início de sessão que estão coladas ao monitor de um computador.
- Os portáteis ou computadores de secretária obsoletos são doados a instituições de caridade sem que tenha sido feita uma limpeza total dos discos rígidos.
- O consultório de um médico é encerrado e os registos dos pacientes são deitados ao contentor do lixo sem antes serem destruídos.

Em 2016, os piratas informáticos comprometeram a segurança de
mil milhões de registos[2]

São cenários como estes que se tornam cada vez mais preocupantes, uma vez que as violações de dados são muito comuns no mundo digital atual. A Forrester reportou que, em 2016, os piratas informáticos comprometeram a segurança de mil milhões de registos em apenas 12 meses. No primeiro semestre de 2017, foi relatado que ocorreram 918 violações de dados que, por sua vez, resultaram em 1,9 mil milhões de registos de dados comprometidos em todo o mundo. Isto representa um aumento de 164 por cento, em comparação com os primeiros seis meses de 2016.[2]

Quando ocorrem novas violações de dados, aumenta o sentimento de ansiedade perante a perda de privacidade dos dados. De acordo com um estudo recente, as pessoas consideram que a sua privacidade está à mercê de problemas de segurança e de confidencialidade. Na realidade, 91 por cento das pessoas receiam que perderam o controlo no que respeita à recolha e utilização dos seus dados por parte das empresas. Um número praticamente igual de pessoas acredita que seria muito difícil remover informações incorretas sobre si do mundo online.[3] Não são apenas as grandes violações de segurança que são uma preocupação. As pequenas empresas podem ter menos informações acerca de um indivíduo, mas o problema não é menos importante se essas informações forem roubadas ou utilizadas indevidamente.

Estes receios continuam a aumentar, apesar de existirem diretivas e regulamentos rígidos no âmbito da privacidade e da proteção dos dados há mais de uma década. A Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), a lei The Fair Credit Reporting e a Diretiva relativa à Proteção de Dados da União Europeia são alguns dos exemplos mais relevantes.

A Diretiva relativa à Proteção de Dados estabelece princípios que ditam, por exemplo, que se deve proteger os dados, que estes devem ser processados para finalidades limitadas e não devem ser mantidos por períodos superiores ao necessário. Contudo, como se trata de uma "diretiva" e não de uma lei, a sua implementação e aplicação variam em cada país europeu.

A entrada em vigor do GDPR
O GDPR é o regulamento mais abrangente e com maior impacto a nível global no âmbito da proteção dos dados pessoais. Foi criado com base na crença partilhada de que todos os indivíduos têm o direito fundamental à privacidade. O seu objetivo é proteger a privacidade dos indivíduos na UE através da aplicação de um novo regulamento que dita a forma como as empresas protegem, processam e utilizam os dados pessoais.

O GDPR poderá ser o avanço mais importante no âmbito da regulamentação da segurança e privacidade de dados dos últimos 20 anos, seja por estabelecer requisitos de responsabilização quanto à manutenção dos registos, seja pelos seus potenciais impactos a nível financeiro. Com dois escalões de multas, as organizações podem ser penalizadas em 2 por cento do respetivo volume de negócios anual a nível mundial ou em 10 milhões de euros por violações como:

- a falha em notificar uma autoridade de supervisão e os indivíduos afetados acerca de uma violação dos dados;
- a falha em designar um encarregado da proteção de dados (EPD) se a organização necessitar de um.

As organizações podem ser alvo de uma coima de 4 por cento do respetivo volume de negócios anual a nível mundial/20 milhões de euros por violações como:

- a falha em honrar os direitos do titular dos dados;
- a falha em atuar em conformidade com uma ordem emitida por uma autoridade de supervisão;
- a falha em cumprir com os requisitos para transferências de dados a nível internacional[4].

Estas coimas são sanções adicionais à perda de reputação, valor da marca e confiança, que podem ser igualmente devastadores para os resultados da empresa. De facto, os incidentes de violação de dados levam a que cerca de 65 por cento dos indivíduos alegadamente percam a confiança na organização em que ocorreram.[5]

A atuação em conformidade com o GDPR não é uma tarefa fácil, uma vez que responsabiliza as organizações quanto aos seus métodos de recolha, utilização, manutenção e eliminação

O GDPR é o regulamento mais abrangente e com maior impacto a nível global no âmbito da proteção de dados pessoais.[1]

dos dados pessoais, mantendo-os protegidos. Mesmo as organizações com programas de privacidade e segurança em vigor necessitam de reavaliar os seus processos. O GDPR exige especificamente que as organizações implementem medidas técnicas e organizativas adequadas para evitar a perda de ou o acesso não autorizado aos dados pessoais.

Neste sentido, colocam-se várias questões como, por exemplo:

P.: O que são dados pessoais?
R.: Todas as informações relativas a uma pessoa singular identificada ou identificável.[6] Pode incluir identificadores (como um nome ou um número de identificação) ou dados reveladores da origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, informação médica, registo criminal, previsões de desempenho laboral, situação económica, interesses ou preferências pessoais, fiabilidade ou comportamento, localização ou movimentações, etc.[7]

P.: O que é a pseudonimização e por que motivo é importante?
R.: O termo "pseudonimização" é mencionado 15 vezes no GDPR e consiste num procedimento em que os campos identificadores de um registo de dados são substituídos por um ou mais identificadores artificiais ou pseudónimos. O GDPR recomenda a aplicação da pseudonimização aos dados pessoais para reduzir os riscos para os titulares dos dados e para ajudar os controladores e subcontratantes a cumprirem com as respetivas obrigações no âmbito da proteção de dados.[8]

P.: As organizações podem obter o consentimento dos indivíduos para recolher os seus dados pessoais?
R.: Sim, mas o consentimento tem de ser dado mediante uma declaração clara e afirmativa, que estabeleça uma manifestação de vontade livre, específica, informada e inequívoca pela qual o titular dos dados aceita o processamento dos seus dados pessoais. Caixas previamente assinaladas, o silêncio e a inatividade não constituem consentimento.[9] As organizações devem manter um registo do consentimento recebido e certificar-se de que os pedidos de consentimento são distinguíveis de outros pedidos, através de linguagem clara e simples.[10] O Artigo 13 descreve **informações amplas** que devem ser facultadas ao titular dos dados no momento em que os respetivos dados são recolhidos, como a finalidade da recolha das informações, os destinatários ou as categorias de destinatários dos dados pessoais e o período de tempo durante o qual os dados serão armazenados.

P.: O que é uma avaliação do impacto sobre a proteção de dados?
R.: Uma DPIA, necessária para atividades de risco elevado, ajuda as organizações a avaliarem a origem, natureza, particularidade e gravidade dos riscos e a implementar medidas adequadas para mitigar os riscos, como a encriptação. Numa avaliação de risco de segurança dos dados, devem ser considerados os riscos apresentados pelo processamento dos dados pessoais, como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou acesso não autorizados, de dados pessoais transmitidos, armazenados ou de outra forma processados, que possa originar danos físicos, materiais ou não materiais.[11]

P.: É necessário designar um encarregado da proteção de dados (EPD)?
R.: A designação de um EPD é obrigatória sempre que o processamento dos dados for efetuado por uma autoridade pública (excetuando os tribunais no exercício da sua função judicial) ou por uma empresa cujas atividades principais consistam em operações de processamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala. A designação de um EPD também é obrigatória para todas as empresas que processam dados relativos a informações sensíveis em grande escala, tais como dados de saúde, convicções religiosas ou políticas. Concretamente, o EPD:

- deve ser designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio das práticas e da legislação sobre proteção de dados;
- pode ser um elemento do pessoal ou um prestador de serviços externo;
- as respetivas informações de contacto têm de ser disponibilizadas à APD;
- tem de ter acesso aos recursos adequados ao exercício das suas funções e à manutenção dos seus conhecimentos especializados;
- tem de responder diretamente ao mais alto nível de administração;
- não pode realizar quaisquer outras tarefas que possam resultar num conflito de interesses.[12]

Requisitos físicos ao nível da privacidade e segurança
O que devem as organizações fazer no sentido de impedir as violações de dados? O Artigo 24 do GDPR estabelece que uma organização é responsável pela implementação de "medidas técnicas e organizativas adequadas" para assegurar e demonstrar que o processamento dos dados pessoais é efetuado corretamente. O Artigo 32 é mais detalhado e explica que "Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo processamento, em particular, devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, armazenados ou, de outra forma, processados".

Um dos aspetos importantes deste regulamento reside na ênfase em impedir o acesso não autorizado. Neste ponto, a segurança física é essencial. Especificamente, pode ajudar a proteger os dados contra ameaças humanas internas e externas cujo objetivo seja tirar partido das falhas na estrutura física da sua organização e através da sua força de trabalho. Isto inclui limitar os dados que podem ser observados, roubados ou acedidos. Analise os pontos seguintes e avalie se a sua força de trabalho aplica as medidas técnicas e organizativas adequadas no sentido de atuar em conformidade.

Implemente a proteção de dados como conceito e como predefinição:
Para proteger os dados por predefinição, as organizações têm de identificar e recolher proativamente apenas os dados pessoais necessários para as respetivas finalidades, preservá-los apenas durante o tempo necessário (princípio da minimização) e garantir que os dados pessoais não serão disponibilizados a um número indefinido de pessoas. É provável que isto inclua garantir que os riscos de privacidade são identificados com antecedência e que os sistemas estão concebidos para mitigar estes riscos, implementar a pseudonimização e a anonimização conforme adequado, criar transparência nas funções de processamento e identificar pessoas ou funções específicas que necessitam de aceder aos dados. Pergunte a si próprio: antes de conceber os seus sistemas de informação, práticas empresariais e estruturas físicas, tem em consideração os riscos de privacidade que podem afetar os indivíduos? Já se reuniu com a sua equipa de TI para analisar os sistemas e as atividades de processamento atuais e para debater se são necessárias medidas adicionais para documentar os métodos de proteção dos dados pessoais ao longo de todo o ciclo de vida dos mesmos?

Utilize as salvaguardas físicas:
Os controlos de cibersegurança, tais como a encriptação dos dados e a utilização de palavras-passe complexas, são aspetos extremamente importantes, mas os controlos físicos e administrativos de "baixa tecnologia" são igualmente importantes. Para determinar os locais onde são necessárias barreiras físicas, identifique os pontos onde é possível aceder a informações sensíveis. Por exemplo, os funcionários utilizam frequentemente os dispositivos móveis para aceder e partilhar dados em qualquer local. Cada vez mais trabalhadores acedem a informações sensíveis em espaços públicos, muitas vezes à vista de terceiros. O risco de exposição dos dados também é elevado dentro do local de trabalho. As disposições de escritórios de espaço aberto comum eliminam as barreiras físicas que tradicionalmente contribuíam para proteger os ecrãs dos computadores. Pergunte a si próprio: posicionou os ecrãs dos computadores longe de janelas, portas e áreas publicamente acessíveis? Os monitores e os ecrãs dos dispositivos móveis estão equipados com protetores de privacidade para obscurecer a visualização das informações por parte de potenciais observadores? As impressoras/fotocopiadoras/máquinas de fax partilhadas estão em áreas protegidas ou têm tampas com fecho de bloqueio? Armazena cópias físicas de dados em instalações com acesso controlado? As destruidoras de papel são equipamentos comuns em todas as unidades no local, especialmente junto a fotocopiadoras, impressoras e faxes? São um pré-requisito para todos os funcionários que estão em regime de teletrabalho ou que utilizam ligações remotas para aceder aos ativos de informações empresariais?

Programe formações para os funcionários:
Os programas de formação deverão abranger três aspetos-chave: Observação, Acesso físico e melhores práticas de Prevenção de roubo. Por exemplo, os funcionários devem estar cientes do que os rodeia quando gerem e acedem a dispositivos ligados em locais públicos através dos seus portáteis, tablets e smartphones. Os ecrãs dos dispositivos não devem estar expostos a quem passa e a potenciais observadores, especialmente quando está a introduzir informações de início de sessão ou a visualizar informações de conta sensíveis. No que respeita ao acesso físico, as organizações devem dar formação aos funcionários no sentido de limpar informações dos quadros brancos e recolherem documentos confidenciais após reuniões, memorizar as palavras-passe em vez de as escrever, trancar os armários de ficheiros e portáteis, utilizar filtros de privacidade em dispositivos informáticos e manter uma política de secretária limpa, incluindo terminar sessão nos dispositivos que não estão em utilização. Pergunte a si próprio: o seu programa de formação envolve a sensibilização situacional dos funcionários para que possam aprender a estar conscientes do ambiente que os rodeia e poderem identificar e atuar perante comportamentos suspeitos? Os funcionários compreendem as expetativas da organização no âmbito da política de "secretária limpa"? Está constantemente a relembrar os funcionários das práticas de segurança recomendadas que devem seguir?

Desenvolva políticas claras:
Para uma organização demonstrar o seu compromisso para com a implementação de medidas de segurança e privacidade adequadas, as respetivas políticas devem descrever o que fazer e não fazer no âmbito da visualização e utilização de informações por parte dos funcionários e dos prestadores de serviços, tanto no local de trabalho, como em situações de trabalho remoto. Os contratos dos funcionários devem incluir linguagem específica acerca da responsabilidade de proteção de informações sensíveis e confidenciais.[13] Pergunte a si próprio: já comunicou a sua declaração de práticas de privacidade e segurança aos seus colaboradores, onde explica como a sua organização protege, partilha, elimina e concede acesso a dados pessoais? Dispõe de uma política de BYOD ("Bring Your Own Device" – Traga o seu próprio dispositivo) que regula a conduta dos funcionários e os controlos de segurança de segurança exigidos quando acedem a recursos da empresa a partir dos dispositivos pessoais? A sua política de segurança exige que os funcionários utilizem controlos visuais e de cibersegurança?

Estabeleça limites para o armazenamento de dados:
Estabeleça limites de tempo para o armazenamento de dados pessoais, em conformidade com a legislação aplicável. Elimine com segurança todos os dados pessoais que não sejam absolutamente necessários para suportar as finalidades empresariais para as quais foram recolhidos. Pergunte a si próprio: que controlos técnicos estão implementados para que os dados sejam eliminados no momento certo? Os processos de destruição dos dados da sua organização respeitam diretrizes de segurança sólidas como, por exemplo, a destruição física de discos rígidos que atingiram o fim de vida útil, conforme indicado na publicação especial 800-88 do Instituto Nacional de Normas e Tecnologia dos EUA?

Verifique a fiabilidade de fornecedores externos: Recorra apenas a subcontratantes que lhe ofereçam garantias suficientes em termos de conhecimento especializado, fiabilidade e recursos para a implementação de medidas organizativas, inclusive ao nível da segurança do processamento. Pergunte a si próprio: dispõe de um programa de gestão de fornecedores que contempla obrigações contratuais e que estabelece atividades de supervisão de gestão de terceiros com acesso a dados pessoais?

Crie um protocolo para violações de dados: As organizações têm de estar preparadas para notificar a autoridade de supervisão, sem atraso indevido, sempre que detetarem a ocorrência de uma violação dos dados pessoais (sempre que possível, num prazo nunca superior a 72 horas). Em alternativa, deverão ser capazes de demonstrar que a violação dos dados pessoais dificilmente resultará em riscos para os direitos e liberdades das pessoas singulares. Se o risco for elevado, os titulares dos dados também têm de ser notificados da violação dos dados sem atraso indevido.[14] Pergunte a si próprio: Quando é que analisou pela última vez os planos e políticas de notificação de violações de dados e de resposta a incidentes da sua organização? Os funcionários sabem quem devem alertar, no seio da organização, se a segurança dos seus dispositivos for comprometida ou se detetarem uma violação dos dados? Existe um plano de notificação de violações de dados e de resposta a incidentes atualizado em vigor que indique quando e como notificar as autoridades acerca de uma violação dos dados?

Conheça os direitos dos indivíduos: Atualmente, os residentes na UE têm o direito de aceder aos dados pessoais que as organizações têm sobre si, bem como o direito de solicitar a eliminação dos mesmos ao abrigo de determinadas circunstâncias. O direito à eliminação exige que as organizações eliminem quaisquer ligações para esses dados pessoais ou cópias ou reproduções dos mesmos. As organizações devem fornecer um método através do qual os titulares dos dados possam apresentar pedidos por via eletrónica, especialmente se os dados pessoais também forem processados por essa via.[15] Pergunte a si próprio: A sua organização compreende o conceito de "dados pessoais" e sabe como responder a pedidos de informação relativos a tais dados?

Conclusão:

O GDPR é a alteração mais importante na regulamentação da privacidade dos dados dos últimos 20 anos. Exige que a gestão dos dados pessoais seja efetuada com vista a garantir os níveis de segurança e confidencialidade adequados, uma tarefa que exige a implementação de medidas de segurança técnicas e organizativas. Além disso, as coimas aplicadas pela não conformidade podem ser devastadoras. Contudo, as melhores práticas descritas no regulamento tratam-se apenas de uma boa conduta empresarial. Nenhum indivíduo quer que os seus dados sejam indevidamente utilizados e nenhuma organização pretende enfrentar as repercussões resultantes de uma violação de dados. As organizações que encaram a privacidade como uma responsabilidade empresarial e não como um fardo relativo à conformidade podem utilizá-la como uma vantagem estratégica para melhorar a sua reputação e o valor da marca, para atrair funcionários de melhor qualidade e, em última instância, preservar a confiança a nível do público.

www.3m.com.pt/filtrosdeprivacidade

[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9 de janeiro de 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Artigo 83 do GDPR, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, patrocinado pela Centrify, 2017.
[6]Artigo 4 do GDPR, 2017
[7]Considerando 75 do GDPR, 2017
[8]Considerandos 26 e 28 do GDPR, 2017
[9]Considerando 32 do GDPR, 2017
[10]Artigo 7 do GDPR, 2017
[11]Artigo 35 e Considerandos 83-84 do GDPR, 2017
[12]Artigos 37-38 do GDPR, 2017
[13]Considerandos 74, 77-78 do GDPR, 2017
[14]Considerando 81 do GDPR, 2017
[15]Considerando 59, 63, 65, 66 do GDPR, 2017

The experts in screen privacy. | 3M