AFRAC

LGPD

Impactos da LGPD nas software-houses

1ª edição/versão – Jan/2021

AFRAC - 2020

SUMÁRIO
LGPD

1. INTRODUÇÃO

A conhecida expressão “Data is the new oil”, que numa tradução livre seria “Dados são o novo petróleo” é atribuída a Clive Humby, um matemático londrino especializado em ciência de dados, tem sido constantemente citada no mercado para demonstrar a ideia de que os dados são tão valiosos quanto o petróleo.

Como se sabe, dados são apenas dados. Entretanto, o grande diferencial ou efeito realmente transformador está na capacidade de analisá-los e tratá-los. E monetizar a quantidade expressiva de dados gerados na Big Data se tornou o desafio e principal modelo de negócio de diversas empresas.
Neste cenário que a proteção de dados ganhou destaque. Aparentemente, pois, o assunto vem sendo discutidos há décadas.

Resumidamente, as primeiras normativas surgiram na Alemanha em meados de 1970 e em outros países da Europa na década seguintes, tendo em vista o avanço da computação e da indústria nos países mais desenvolvidos.

Já em 1995, mesmo com a Internet ainda incipiente, a União Europeia estabeleceu a Diretiva 95/46/CE unificando as normas existentes, definindo conceitos e estabelecendo princípios e obrigações.

Avançando na legislação de proteção de dados e economia digital, a União Europeia endureceu a regulação aprovando em 2016 o Regulamento Geral de Proteção de Dados 2016/679, conhecido como General Data Protection Regulation (GDPR). O GDPR entrou em vigor em maio de 2018.

No Brasil, apesar de legislação específica só vir à tona em 2018, nossa Constituição Federal de 1988 tratou, ainda que de forma geral, da privacidade dos cidadãos. Depois, tivemos algumas garantias relacionadas aos consumidores no Código de Defesa do Consumidor (1990) e a publicação do Marco Civil da Internet (Lei nº 12.965/2014).

Com a sombra do GDPR Europeu repercutindo globalmente e nas empresas brasileiras, foi publicada em agosto de 2018 a Lei Geral de Proteção de Dados (Lei nº 13.709) que dispõe “sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

Para proteger as operações de tratamento de dados, a lei considera tratamento toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (artigo 5º, inciso X, da Lei nº 13.709/2018).

Em outros termos, a LGPD é uma lei que busca garantir a segurança de dados pessoais, respeitando a liberdade individual e a privacidade de cada um.

A LGPD se aplica a toda qualquer operação de tratamento realizada para fins econômicos ou comerciais, online e/ou off-line, por qualquer pessoa, seja natural ou jurídica, de direito público ou privado, não apenas às empresas localizadas no Brasil, mas também àquelas que oferecem serviços ao mercado consumidor brasileiro ou coletam e tratam dados de pessoas localizadas no país.

Depois de idas e vindas, a Lei 13.709/2018 passou a vigorar em 18 de setembro de 2020, com suas penalidades prorrogadas para aplicação em agosto de 2021.

Entretanto, apesar de postergada a vigência das penalidades, com fiscalização e aplicação pelo órgão adequado, no caso a Autoridade

Nacional de Proteção de Dados (ANPD), nada impede que outras instituições e órgãos de controle possam atuar e multar, como Procon, Ministério Público, com base nas exigências contidas na LGPD.

Assim, todos aqueles que participam do ecossistema que envolve a proteção de dados pessoais devem estar cientes de seus direitos e deveres, finalidade, inclusive, desta cartilha que permitirá, sem esgotar o assunto, conhecer os principais pontos e desafios da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

2. SEGURANÇA DE BANCO DE DADOS
O QUE DIZ A LEI

Art. 5º Para os fins desta Lei, considera-se:

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

A criação e manutenção de um banco de dados eletrônico deve preceder de uma série de estudos, cuidados e boas práticas para que se tenha a segurança necessária para o atendimento da Lei 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Necessário, também, os cuidados com a infraestrutura tecnológica onde este banco de dados estará hospedado.

A LGPD, ainda dispõe:
Art. 6º *As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
...
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
...
Art. 46. *Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito*

IMPACTOS PARA AS SOFTWARE-HOUSES

Dentro do ciclo de vida do tratamento dos dados pessoais, destacaremos neste item a RETENÇÃO, que equivale ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado. Aqui trataremos a retenção dos dados em um banco de dados eletrônico SGBD – em nuvem ou não.

Os artigos 6º e 46 estipulam a necessidade da adoção de medidas técnicas para proteção dos dados de forma ampla. Embora essa obrigação seja especificada para os agentes de tratamento (controlador e operador), não há dúvidas de que é o operador (a software-house) quem detém as ferramentas e os meios para a implementação da maioria das medidas de segurança no banco de dados. Ao controlador cabe a responsabilidade de cobrar do operador que lhe forneça os mecanismos necessários (ou contrate outro operador que o faça), bem como garantir a infraestrutura necessária e compatível com a segurança da informação armazenada.

O QUE FAZER NA PRÁTICA

Há inúmeras medidas técnicas e administrativas que visam aumentar a segurança da informação armazenada no banco de dados e prevenir o acesso de um oponente mal intencionado. Considere os seguintes tópicos como ponto de partida na avaliação de segurança oferecida pela sua solução.

Leve em conta que muitos dos tópicos abaixo requer não somente a execução mas a criação, registro e manutenção de uma política (documento interno com diretrizes para a organização) que dê suporte às ações.

Segurança física

- Controle de acesso físico aos servidores de banco de dados e demais equipamentos de infraestrutura.
- Execução dos backups regulares com testes de recuperação.
- Controle de acesso as mídias dos backups.
- Se o armazenamento for em "nuvem" é necessário considerar o serviço de armazenamento utilizado e definir os requisitos mínimos que o prestador do serviço garante.

Segurança lógica

- Não utilização de senhas padrões dos fabricantes dos equipamentos.
- Atualização permanente dos hardwares e firmwares.
- Utilização de softwares atualizados e legalizados do SO, SGBD, acesso remoto, antivírus e outros.
- Controle de acesso remoto aos servidores.

Banco de dados

• Utilização de SGBD com configuração mínima que assegure controle e restrição de acesso;

• Utilização, sempre que possível, de usuários nomeados.

• Não utilização de senhas padrões no banco de dados.

• Definição de política de senhas fortes para acesso ao BD.

• Se possível, limitar o acesso direto ao banco de dados por operadores não logados no sistema.

• Utilizar recursos para limitar os privilégios de usuários.

• Avaliar os direitos de acesso dos usuários altamente privilegiados, tais como DBAs, usuários de aplicação e administradores de sistema.

• Utilização de criptografia para a garantia da confidencialidade, sempre que necessário (ver capítulo sobre criptografia nesta cartilha).

• Não utilizar bancos de dados em produção (ou mesmo suas cópias) para tarefas de desenvolvimento e testes.

ONDE OBTER
MAIS INFORMAÇÕES

GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – www.gov.br

Oracle - oracle.com.br

Boas Práticas em Segurança da Informação – Portal tcu.gov.br

Família de normas ABNT ISO/IEC 27000

3. SENHAS, GESTÃO DE USUÁRIOS E PERMISSÕES DE SISTEMA

O QUE DIZ A LEI

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

IMPACTOS PARA AS SOFTWARE-HOUSES

A gestão de permissão de usuários tem papel central na proteção de dados e gestão de privacidade. É sabido que grande parte dos ataques são viabilizados explorando comportamentos inadequados, falta de conhecimento ou a inércia do usuário. Não fosse assim, nenhum usuário utilizaria senhas como 123456 (uma das senhas mais comuns em sistemas que permitem a utilização de senhas sem requisitos mínimos de segurança). Cabe ao desenvolvedor de software “conduzir” o usuário (as vezes de forma coercitiva) a utilização de boas práticas de segurança.

O QUE FAZER NA PRÁTICA

Há inúmeras providências que podem ser utilizadas para a gestão segura de senhas e usuários. Deixamos uma lista de sugestões a ser considerada abaixo.

1. Implementação de uma política de validade de senhas compatível com os requisitos de segurança da sua solução. Ex: As senhas devem possuir validade de 90 dias, após passar o prazo os sistemas devem solicitar automaticamente a troca de senha, sempre alertando com antecedência à expiração da mesma;

2. Utilização de uma política de comprimento mínimo de senhas. Como regra básica considere que senhas com menos de 8 caracteres podem deixar a desejar em termos de segurança, independentemente da sua composição;

3. Implementação de uma política que impeça o reaproveitamento de senhas (utilização de senhas utilizadas anteriormente);

4. Bloqueio de conta após uma quantidade de tentativas inválidas. O bloqueio pode ser temporal (por “x” minutos) ou até que a redefinição por um método seguro (um e-mail de reset de senha, por exemplo);

5. Bloqueio de senhas contendo nome ou parte do nome do usuário, ou dados associados ao cadastro do usuário (datas de nascimento, etc.);

6. Bloqueio de senhas com sequências de caracteres, números ou letras;

7. Bloqueio e senhas que utilizem informações da empresa em que trabalha para compor senha.

4. UTILIZAÇÃO DE CRIPTOGRAFIA

O QUE DIZ A LEI

A palavra “criptografia” não aparece em nenhum dos 65 artigos da LGPD. Apesar disso, ela é uma das ferramentas técnicas mais importantes para a garantia da segurança e privacidade de dados e, praticamente, uma obrigação do desenvolvedor de software. O artigo 46º da LGPD diz textualmente:

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Não há dúvida que umas das ferramentas mais eficazes para a proteção de dados contra acesso não autorizado é a criptografia.

IMPACTOS PARA AS SOFTWARE-HOUSES

É claro que a utilização da criptografia deve ser feita dentro de um contexto de estratégia de segurança, pois nenhuma medida isolada é capaz de prover a proteção necessária aos dados. Em outras palavras: o uso indiscriminado de criptografia no seu sistema pode trazer impactos negativos à usabilidade e o desempenho e não vai resolver o “assunto” LGPD. Ao contrário, o desenvolvedor de software deve considerar os cenários em que a utilização de criptografia pode ajudar.

O QUE FAZER NA PRÁTICA

Entre as técnicas de criptografia que podem ser consideradas pelo desenvolvedor de software, estão:

Criptografia em repouso.

A criptografia em repouso pode ser utilizada no contexto do sistema operacional ou do banco de dados e garante que as informações são gravadas na mídia física de forma criptografada, incluindo as mídias de backup. A utilização dessa técnica tem como principal função evitar que a perda ou furto de mídias contendo dados pessoais (ou de negócios) comprometam a segurança da informação.

O recurso de criptografia em repouso mais conhecido (no ambiente Windows) é o Bitlocker, mas existem diversas ferramentas disponíveis para essa função em outros sistemas operacionais. No contexto do banco de dados, a maioria dos SGBDs possui ferramentas de criptografia em repouso que valem a pena ser considerados. A criptografia em repouso não impede o acesso às informações do banco de dados para o oponente que tem as credenciais de acesso ao banco de dados.

Criptografia de informações no banco de dados.

Manter as informações criptografadas no banco tem um propósito diferente da criptografia em repouso. Ela visa impedir a obtenção de informações mesmo quando o invasor possui acesso ao banco de dados (como usuário administrador do sistema ou do SGBD). Neste caso, os dados só são possíveis de interpretação com a chave criptográfica adequada que pode estar armazenada de forma inacessível ao invasor mas acessível ao software de gestão. Existem diversas técnicas de criptografia de informações utilizando chaves públicas ou privadas, que estão fora do escopo desta cartilha. Mas cabe ressaltar que, mais uma vez, os SGBDs modernos possuem ferramentas nativas para a gravação/recuperação de dados de forma criptografada.

Mascaramento de dados.
Embora não se trate exatamente de uma criptografia, o recurso de mascaramento de dados pode ser útil no conjunto de medidas de proteção que podem ser utilizadas.

O mascaramento de dados faz com que o usuário sem permissão de acesso completo veja a informação de forma parcialmente oculta.

Exemplo: um número de cartão de crédito
é gravado no banco como abaixo:
4545 4584 5698 4587

Mas, ao ser consultado por um usuário sem as permissões
de acesso total é mostrado da seguinte forma:
45 **** **** *587**

Utilização de Hash.
As funções *hash*, as vezes chamadas de criptografia de mão única, permite a gravação segura de informações que não necessitam ser decifradas. O exemplo mais comum é a persistência de senhas. Em vez de gravar a senha do usuário em formato não cifrado, é gravado o seu hash (normalmente acrescido de um texto adicional como semente de segurança). Então, no momento da autenticação do usuário, compara-se o hash da senha digitada (utilizando o mesmo algoritmo anteriormente usado no cadastro do usuário). A utilidade primária dessa técnica é evitar que dados sensíveis sejam comprometidos mesmo que o invasor tenha conseguido acesso pleno as informações do banco de dados.
Como visto, existem várias técnicas de criptografia disponíveis que podem ajudar a garantir a segurança da informação dos dados no âmbito da LGPD. Cabe ao desenvolvedor de software analisar qual delas (ou qual combinação delas) é a mais adequada para a sua realidade e requisitos de segurança do seu modelo de negócios.

ONDE OBTER MAIS INFORMAÇÕES

Manuais de segurança de informação e livros de criptografia em geral.

5. ANONIMIZAÇÃO E ELIMINAÇÃO DE DADOS
O QUE DIZ A LEI

Art. 5º

...

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

...

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

Art. 12. *Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.*

Art. 16. *Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:*

...

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

...

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Art. 18. *O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*

...

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

IMPACTOS PARA AS SOFTWARE-HOUSES

Se dado pessoal é uma informação relativa a uma pessoa física identificada ou identificável, dados anonimizados são os dados que não podem ser associados a uma pessoa física utilizando os esforços técnicos compatíveis com a realidade tecnológica no momento em que o processo foi executado.

O conceito de dados anonimizado é criado para permitir que os controladores conservem dados que seriam pessoais sem violar a legislação. E qual utilidade há num dado que não é associado a uma pessoa física? Há várias. Esses dados permitem a um lojista conhecer a faixa etária dos seus clientes. Idem para análise de renda ou qualquer outra informação que possa ser relevante, mesmo na ausência da associação individual com o titular. A anonimização é, portanto, uma alternativa legal à disposição do controlador para manter informações sobre titulares (agora não identificados ou identificáveis) ao término do tratamento de dados. Cabe lembrar que dados anonimizados não são considerados dados pessoais.

O desenvolvedor de software que disponibilizar recursos para anonimização de dados de clientes deve estar atento ao fato de que, muitas vezes, o processo de anonimização pode ser revertido pela associação de bases de dados diferentes. Neste caso, não se pode dizer que houve uma anonimização verdadeira compatível com a legislação.

O QUE FAZER NA PRÁTICA

Abaixo vemos um exemplo prático da utilização do processo de anonimização:

Um varejista (controlador de dados) possui um banco de dados de seus clientes (titular dos dados pessoais) visando programas de fidelidade. Nesse caso, ao solicitar o consentimento do cliente a finalidade utilizada foi tão somente o envio de conteúdos promocionais.

Este varejista, agora, pensa em utilizar os dados de venda de suas lojas para seus centros de distribuição e logística focando-se no gênero e idade de seus clientes. Caso ele queira que neste processo o titular de dados seja identificado, ele terá que solicitar um novo consentimento para esta finalidade, visto que a mesma não estava prevista no primeiro consentimento.

Todavia, o varejista (controlador de dados) verifica e conclui que não precisará da identificação do seu cliente para o que pretende, sendo assim, os dados anonimizados não irão impactar na sua finalidade de uso desses dados.

Assim, ele aplicará, através de seu operador, técnicas razoáveis para que possa desvincular a identificação dos dados junto ao titular (clientes).

É importante constar que a aplicação de técnicas atuais de anonimização possam ser atualizadas caso surjam mecanismos técnicos diante da evolução da própria tecnologia que tornariam a reversão simples do processo.

Fonte:
http://genjuridico.com.br/2020/08/05/conceito-anonimizacao-dado-anonimizado/ (Última visualização em 14.10.2020)

ONDE OBTER MAIS INFORMAÇÕES

Sobre as técnicas de anonimização, a LGPD indica que a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Contudo, até o momento da elaboração desse texto, a ANPD ainda não se manifestou a este respeito. Dessa forma, é possível utilizar como fonte de informação o artigo elaborado pela Autoridade de Proteção de Dados do Reino Unido (vide página 80 em diante):

https://ico.org.uk/media/1061/anonymisation-code.pdf

6. OBTENÇÃO E GESTÃO DE CONSENTIMENTOS DOS TITULARES

O QUE DIZ A LEI

Art. 5º

...

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Art. 7º *O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*

I - mediante o fornecimento de consentimento pelo titular;

Art. 8º *O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.*

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Art. 9º *O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:*

...

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Art. 11. *O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. *O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.*

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Seção IV - Do Término do Tratamento de Dados

Art. 15. *O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:*

...

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

Art. 18. *O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*

...

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

...

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Art. 19. *A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:*

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

IMPACTOS PARA AS SOFTWARE-HOUSES

O consentimento do titular é uma das hipóteses legais que permitem ao controlador o tratamento dos dados pessoais. A LGPD dedica vários artigos ao regramento de como deve ser obtido e registrado esse consentimento.

O consentimento que não possa ser demonstrado pelo controlador ou ainda que não tenha sido obtido em conformidade com o regramento é nulo de direito e traz grandes riscos à empresa que dele se utiliza.

O QUE FAZER NA PRÁTICA

Ao controlador cabe o ônus da prova de que um consentimento legítimo foi obtido dos seus titulares. Ao desenvolvedor de software, cabe auxiliar o titular na obtenção e registro dos consentimentos obtidos pelos seus clientes (os controladores) Para isso, podem ser utilizadas várias abordagens, entre elas:

Para softwares com a funcionalidade de gerenciamento de clientes, o sistema deve possuir um controle que permita identificar os clientes que concederam o seu consentimento e aquele que não o fizeram.

Considere registrar a forma como foi obtido o consentimento:

- ELETRÔNICO: para consentimento realizados de forma eletrônica, confirmação por e-mail ou navegador do TITULAR.

- IMPRESSO: para consentimento impressos e assinados pelo TITULAR do dado.

Outros dados que podem ser armazenados como documentação utilizada na prestação de contas pelo controlador:

- DATA E HORA DO CONSENTIMENTO: data e hora que o consentimento foi realizado.

- OPERADOR CONSENTIMENTO: operador do sistema que realizou a interação com o TITULAR para obtenção do consentimento.

- DATA E HORA DA REVOGAÇÃO: data e hora que a revogação foi solicitada pelo TITULAR.

- OPERADOR DA REVOGAÇÃO: operador do sistema que realizou a interação com o TITULAR para obtenção da revogação.

O sistema pode possuir a funcionalidade de impressão do consentimento com o seu respectivo aviso de privacidade em modelo adaptável à necessidade do controlador.

O sistema pode ter opções de envio eletrônico (e-mail ou outras mensagens eletrônicas) do aviso de privacidade e o termo de consentimento que levará o titular a tomar uma ação inequívoca que permite demonstrar a concordância com os termos do consentimento (visita a um link, clique num botão, etc.)

O sistema deve possuir a possibilidade de registrar a revogação do consentimento por parte do titular.

O sistema deve possuir a funcionalidade para eliminar os dados do TITULAR mediante a solicitação.

ONDE OBTER MAIS INFORMAÇÕES

LGPD - Lei Geral de Proteção de Dados

7. GESTÃO DE SOLICITAÇÕES DE CLIENTES

O QUE DIZ A LEI

Art. 18. *O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.(Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

IMPACTOS PARA AS SOFTWARE-HOUSES

O exercício de direitos dos titulares é um dos pontos em que o desenvolvedor de software pode atuar para colaborar na adequação à LGPD por parte dos seus clientes. O exercício de cada direito pode ser exercido de formas diferentes, assim, vale a pena a análise de cada um deles de maneira individual.

O QUE FAZER NA PRÁTICA

1. Art. 18, I - CONFIRMAÇÃO DA EXISTÊNCIA DO TRATAMENTO.

A resposta deve ser providenciada de imediato e em formato simplificado ou por declaração clara e completa, fornecida no prazo previsto em lei e que indique:

• Origem dos dados, a existência de registro, critérios utilizados, finalidade do tratamento.
• Garantir de forma fácil e clara sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência)
• A finalidade do tratamento para propósitos legítimos, específicos.

2. Art. 18, II - ACESSO AOS DADOS.

O titular deve ter livre acesso, garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como a integridade de seus dados pessoais.
Você pode definir qual procedimento de verificação contínua quanto a exatidão, clareza relevância e a atualização dos dados do titular.

Deve-se deixar claro o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).

Acesso a informação sobre a confirmação da existência de tratamento (Art.18, I).
Acesso aos dados coletados (Art. 18, II).

Acesso a informação sobre entidades públicas e privadas com os quais o controlador realizou uso compartilhado de dados (Art. 18, VII).

Nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso a cópia eletrônica integral de seus dados pessoais.

Acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automática.
OBS: Na impossibilidade de retorno imediato o controlador poderá comunicar que não é agente de tratamento de dados e indicar o agente. Ou indicar as razões que o impedem.

3. Art 18, III - CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS.

O titular tem por direito solicitar revisão dos dados e que corrija dados incompletos, ou inexatos ou de mudanças de cadastros, ou de qualquer outra natureza considerado dados pessoais sempre que for necessário de forma clara e rápida.

Os dados pessoais que você fornece podem ser de perfil pessoal, profissional, de consumo ou de crédito, com base nas suas informações e que podem afetar os seus interesses.

Nessas hipóteses, o titular tem direito a obter informações sobre os critérios e procedimentos empregados no processo, além do direito a solicitar a revisão dessas decisões conforme Art. 20.

A revisão em tela, previsto no Art. 22º da GDPR (Regulamentação da União Europeia), implica a revisão por ser humano, para que confirme ou corrija eventuais erros da decisão automática anterior ou de input humano, de forma justificada.

De modo análogo (semelhante), a Lei do Cadastro Positivo já permitia a revisão de decisões (automáticas) pelo consulente das informações cadastrais obtidas em bancos de dados (Lei 12.414/2011, art.5º, VI); naturalmente, a expressão refere-se a pessoa natural.

4. Art. 18, IV – ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS DESNECESSÁRIOS, EXCESSIVOS OU TRATADOS EM DESCONFORMIDADE COM O DISPOSTO NA LGPD.

Segundo a LGPD, sempre que possível, os dados serão anonimizados, ou seja, tratados de forma a não permitir a identificação do titular; dados desnecessários ou excessivos são aqueles que não atendem às finalidades

informadas para o tratamento e, por isso, devem ser eliminados.
OBS: Pseudoanonimização é quando você consegue reverter os dados anonimizados. Portanto, a lei não contempla aqui neste artigo esta possibilidade de reversão.
Se os dados não forem de manutenção obrigatória por exigência legal, o titular tem direito a solicitar sua eliminação, a menos que estejam previstos no Art. 16 desta lei.

Art. 18, VI, c/c 16: De fato, os dados não poderão ser eliminados quando a lei determinar sua conservação para cumprimento de obrigação legal ou regulatória pelo controlador, entre outros casos.
Essa solicitação deverá ser atendida imediatamente, a menos que o requerido não seja o agente de tratamento (sempre que possível ele deverá indicar quem o seja) ou apresente justificativa que impeça a eliminação imediata dos dados (Art. 18, §§ 3º e 4º).

Art.18, §6º: Uma vez requerida a correção, anonimização, bloqueio ou eliminação dos seus dados pessoais, o agente de tratamento deverá providenciar para que medida idêntica seja adotada por todos os demais agentes com quem tenha realizado o uso compartilhado.
OBS: Como este prazo "imediato" nem sempre será possível para algumas empresas, o que alguns aconselham, é colocar estes dados em contrato para deixar claro ao titular que você terá um prazo para entrega. Qual será este prazo? O mais rápido possível. Mas pelo menos ele saberá que você tem um delay de entrega.

5. Art. 18, V – PORTABILIDADE DOS DADOS A OUTRO FORNECEDOR DE SERVIÇO OU PRODUTO, MEDIANTE REQUISIÇÃO EXPRESSA E OBSERVADOS OS SEGREDOS COMERCIAL E INDUSTRIAL, DE ACORDO COM A REGULAMENTAÇÃO DO ÓRGAO CONTROLADOR.

A portabilidade significa que o titular pode levar seus dados para outro fornecedor de serviço ou produto. Para isso deverá fazer requisição expressa, de acordo com a regulamentação da autoridade nacional (e desde que a transferência dos dados não importe em violação de segredos comercial e industrial). Por exemplo, um motorista de aplicativo que deseje mudar de

plataforma poderá levar para o novo serviço as avaliações pelo usuário que foram obtidas na plataforma anterior.
- Será possível se as informações não consistam em algum segredo comercial
- Saber se há ou não portabilidade com organizações privadas ou públicas

6. Art. 18, VI – ELIMINAÇÃO DOS DADOS PESSOAIS TRATADOS COM O CONSENTIMENTO DO TITULAR, EXCETO NAS HIPÓTESES PREVISTAS NO ART. 16 DA LGPD.
Este item foi tratado acima no 4. Art. 18, IV

7. Art. 18, VII – INFORMAÇÃO DAS ENTIDADES PÚBLICAS E PRIVADAS COM AS QUAIS O CONTROLADOR REALIZOU USO COMPARTILHADO DE DADOS. Caso tenha sido compartilhado dados com terceiros como exemplo órgão públicos (Sefaz tramitando XML) e contabilidades (XMLs, Speds, outros dados para legislações obrigatórias), ou arquivos para compatibilidade de ERP, etc.

8. Art. 18, VIII – INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO E SOBRE A CONSEQUÊNCIA DA NEGATIVA.
Há determinados casos onde a negativa do titular quanto ao consentimento possa ensejar em não utilização de determinadas funcionalidades oferecidas pelo serviço ou solução do Controlador. Mais especificamente, o consentimento pode, por exemplo, facultar que determinados dados não sejam cruciais para a usabilidade de determinada ferramenta, porém a ausência do consentimento em determinados dados inviabilizará outras eventuais funcionalidades.

9. Art. 18, IX – OPÇÃO DE REVOGAÇÃO DO CONSENTIMENTO, A QUALQUER MOMENTO, MEDIANTE MANIFESTAÇÃO EXPRESSA POR PROCEDIMENTO GRATUITO E FACILITADA.

FORMULÁRIO DE SOLICITAÇÃO DO TITULAR DE DADOS

IDENTIFICAÇÃO DA ENTIDADE A SER ABORDADA POR ESTE PEDIDO

LOGO DA SUA EMPRESA

IDENTIFICAÇÃO DO TITULAR DE DADOS / REPRESENTANTE

NOME

ENDEREÇO NR.

CIDADE PAÍS

CEP/ UF

TIPO DO DOCUMENTO

TITULAR OU REPRESENTANTE LEGAL

ENVIO DA SOLICITAÇÃO POR MEIO DE: EMAIL [ ] / CARTA [ ] / LIGAÇÃO [ ]

CLIENTE AUTORIZADO ? SIM [ ] NÃO [ ]

SOLICITAÇÕES DO TITULAR :

Art. 18, I: confirmação da existência do tratamento [ ]

Art. 18, II: acesso aos dados [ ]

Art. 18,III: Correção de dados, incompletos, inexatos ou desatualizados : [ ]

Art.18, IV: Anonimização, Bloqueio ou eliminação dos dados: [ ]

Art.18, V: Portabilidade para terceiros: [ ]

Art. 18, VI: Eliminação dos dados pessoais tratados com consentimento do titular: [ ]

Art. 18, VII: Informação das entidades públicas ou privadas que teve compartilhamento: [ ]

Art. 18, VIII: Informação sobre a possibilidade de não fornecer consentimento: [ ]

Art.18, IX : Opção de revogação do consentimento [ ]

Observação livre do titular: [ ]

ASSINATURA DO REPRESENTANTE LEGAL

8. PUBLICIDADE EM GERAL E E-MAIL MARKETING EM PARTICULAR

E-mail marketing e publicidade em geral

Existem duas hipóteses na LGPD para embasar a coleta e o tratamento de dados nos casos de envio de e-mail marketing e de publicidade em geral. São elas: o legítimo interesse do controlador e o consentimento.

Ainda não se pode afirmar com clareza qual será a abordagem da ANPD (Autoridade Nacional de Proteção de Dados) em relação a abrangência do conceito de legítimo interesse, mas o artigo 10º da LGPD, em seu inciso I, deixa explícito que este inclui o apoio e promoção das atividades do controlador.

Ou seja, é possível enquadrar a publicidade e o e-mail marketing no conceito de legítimo interesse desde que os dados utilizados sejam apenas os estritamente necessários para aquela finalidade. Assim, ficam preservados tanto os direitos do titular com relação a seus dados quanto os direitos do controlador de promover suas atividades.

Já com relação ao consentimento, alguns cuidados precisam ser tomados, tais como:

Informar ao titular com clareza por quais meios ele receberá a publicidade (exemplo: por sms, e-mail, telefone, push);

Dar ao titular a opção de aceitar ou não fornecer seus dados (aqui a sugestão é substituir o botão único de aceitação por duas opções, no qual o titular obrigatoriamente precisa se posicionar quanto a aceitação ou não de receber publicidade);

Manter a possibilidade de retirar o consentimento a qualquer momento;
Informar de modo claro ao titular a finalidade do uso dos dados solicitados pela empresa.

9. AUDITORIAS DECORRENTES DA LGPD

A LGPD em sua Seção destinada à Segurança e Sigilo de Dados no Capítulo que traz informações sobre as boas práticas que devem ser observadas pelos agentes de tratamento, indica que os mesmos devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de incidentes ou demais hipóteses de tratamento inadequado ou ilícito.

Na figura do Operador, ou seja, aquele responsável por realizar o tratamento de dados pessoais em nome do Controlador e que, em grande parte, é um parceiro técnico especializado, deve garantir a segurança do tratamento.
Uma das principais formas de demonstrar que adota as medidas técnicas de segurança é a viabilidade de permitir a realização de auditorias por parte do Controlador junto ao Operador.

É sabido que a LGPD foi inspirada no GDPR, este último, por sua vez traz regras específicas sobre a relação entre o Controlador e o Operador, especialmente no tocante a necessidade um contrato ou instrumento legal para formalizar a relação de tratamento de dados efetuada pelo Operador em nome do Controlador.

A previsão no GDPR sobre a necessidade do contrato está prevista no artigo 28, parágrafo 3º. Dentre os itens destacados nessa lei que são necessários no contrato o item “h” dispõe (tradução livre):

3. O tratamento por um OPERADOR deve ser regulado por contrato ou outro ato legal determinado pela União ou lei do Estado-Membro, que vincule o OPERADOR ao CONTROLADOR e que estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do CONTROLADOR. Esse contrato ou outro ato legal deve estipular, especificamente, que o OPERADOR:
(...)

h) Disponibiliza ao CONTROLADOR todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e permite e contribui para as auditorias, inclusive as inspeções, conduzidas pelo CONTROLADOR ou por outro auditor em seu nome.

Entendemos que a viabilidade em permitir e apoiar a realização de auditorias por parte do Controlador certamente demonstra que o Operador adota boa prática de medidas de segurança e administrativas.

É interessante pontuar que em pesquisa aos contratos de tratamentos de dados elaboradores por Operadores (ou Processadores) que submetem-se ao GDPR, estes indicam prazos específicos e os modos de realização da auditoria, destacando períodos mínimos de avisos por parte do Controlador, assim como garantias de confidencialidade de relatórios.

10. QUESTÕES CONTRATUAIS ENTRE OPERADOR E CONTROLADOR

Este capítulo serve como orientações gerais sobre as principais boas práticas e aspectos de observância para a empresa desenvolvedora de software, quando esta figurar como operadora em suas relações comerciais, no que tange aos contratos que irão nortear sua relação com o cliente, esse último, por sua vez, figurar como controlador, do ponto de vista da Lei Geral de Proteção de Dados.

Reforçamos que este material não possui natureza de assessoria jurídica e, portanto, recomendamos que as empresas busquem orientação profissional do advogado para a redação adequada de seus contratos, especialmente considerando que a sistemática da solução e operação da empresa muitas vezes é diferente e deve ser analisada de forma específica.
A LGPD não dispõe expressamente sobre a obrigatoriedade do contrato entre controladores e operadores.

Por outro lado, o GDPR - General Data Protection Regulation – Regulamento Geral de Proteção de Dados, legislação da União Europeia que visa a proteção dos dados pessoais, dispõe expressamente essa necessidade através do seu artigo 28, parágrafo 2º, pormenorizando, inclusive, algumas cláusulas essenciais que deverão conter no instrumento.
Reforçamos que a criação da LGPD no Brasil foi fortemente inspirada nessa legislação europeia.

Mas não é apenas nela que identificamos a necessidade do contrato, normas como a ISO 27.701, uma extensão da norma ISO 27001, traz parâmetros de sistema de gestão de segurança privada e, especificamente, dispõe sobre os Controles aos Controladores de Dados (Anexo A), ao indicar que a organização deve possuir um contrato por escrito com qualquer operador de Dados Pessoais que ela utilize.

Dessa forma, apesar de não haver previsão expressa na LGPD sobre a

necessidade de um contrato por escrito entre controlador e operador, pela leitura dessa própria norma identifica-se inúmeros fatores que permitem concluir que o instrumento por escrito é importante, necessário e se mostra uma das medidas administrativas para garantia da segurança quanto ao processo de tratamento de dados pessoais (artigo 46/LGPD).

Sob o ponto de vista do GDPR, os contratos dessa natureza são denominados DPA (Data Processing Agreement), em sua versão brasileira, muitos os têm denominado como Acordo ou Contrato de Processamento/Tratamento de Dados.

Em apurada leitura da LGPD e contemplando as determinações do GDPR, concluímos que os contratos entre Controladores e Operadores devem focar-se em alocação das responsabilidades de cada parte (considerando a natureza da relação e as funcionalidades da solução de software oferecida).
Dentre os diversos pontos a serem considerados quando da elaboração de contratos dessa natureza, apontamos alguns exemplos e sua necessidade de reflexão:

- Atendimento de Solicitação aos Titulares de Dados: Apesar de tal responsabilidade estar indicada na LGPD como exclusiva ao Controlador, é importante refletir as funcionalidades e entregas de cada solução, assim como o comportamento quanto ao atendimento a ser realizado, seja na exclusão dos dados a partir de pedido do titular, especialmente em se tratando de soluções que contemplem backup dos dados, ou até mesmo em correções dos mesmos.

- Término do Tratamento de Dados: Orientamos ser importante a definição expressa dos processos relacionados ao término da relação comercial (entre controlador e operador), procedimentos e previsões da forma como se dará a exclusão ou devolução dos dados.

- Instruções do Controlador: Dentre as responsabilidades disciplinadas aos

agentes de tratamento pela LGPD, destaca-se a obrigação exclusiva do Operador no que tange a observância das instruções lícitas do Controlador quanto ao tratamento dos dados.

O não cumprimento da instrução lícita do Controlador, ou até o mesmo o cumprimento de instruções do Controlador que são reconhecidas como ilícitas por parte do Operador ensejarão em responsabilidade e eventual ressarcimento caso haja ocorrência de dano ao titular.

Desta forma, reforça-se a importância e constar no contrato as instruções iniciais do Controlador junto ao Operador, a fim de mitigar suas responsabilidades, sendo que novas instruções possam tão somente, se possível, serem dadas mediante procedimentos formalizados, para que se garanta a comprovação por parte do Operador que suas atividades de tratamento não escapam das finalidades e propósitos atribuídos pelo Controlador.

Ainda no que tange as instruções do Controlador como ponto a ser firmado em instrumento contratual, também sugerimos que haja previsão quanto aos procedimentos que serão adotados por parte do Operador quando da verificação de que determinada instrução possa estar violando a legislação de proteção de dados, seja através da comunicação imediata e interrupção das atividades até o efetivo esclarecimento ou ajustes necessários.

Por fim, sugerimos a inserção de eventuais cláusulas quanto a Suboperadores (especialmente em empresas que subcontratam serviços de armazenamento em nuvem), indicando as autorizações quanto a eventuais suboperadores listados e indicados, o procedimento quanto a eventual adição ou retirada de uma das empresas listadas e, em especial, se há transferência internacional de dados.

Pontuamos que no tocante a transferência internacional de dados, a LGPD deixa a cargo da ANPD vários procedimentos e apontamentos que estão pendentes de regulamentação e/ou informação desta Autoridade.

No entanto, acreditamos que a previsão desde já nos contratos entre Operadores e Controladores acerca desse tema mereça ser realizada, onde destacamos a possibilidade de apontamentos dos países onde ocorrerá a transferência internacional.

É importante lembrar que a LGPD cita as hipóteses taxativas para a ocorrência da transferência internacional de dados, desta maneira, cabe a parte entender se observa uma das hipóteses e adaptar seus contratos de acordo com a hipótese a que está sendo fundamentada a transferência.

Reforçamos, por fim, a análise de demais fatores a serem considerados e ajustados em contratos, seja através de anexos contemplando medidas de segurança adotadas pelo Operador; destaques quanto a medidas administrativas adequadas para aqueles que eventualmente terão acesso aos dados quando da atividade do tratamento (como cláusulas assegurando observâncias a acordos de confidencialidade, códigos e políticas internas de segurança).

AFRAC

www.afrac.org.br

R. Prof. Aprígio Gonzaga, 35 · Conjunto 64
São Judas, São Paulo - SP, 04303-000