A LGPD e os Provedores de acesso à internet

Esse documento foi elaborado com a finalidade de servir como cartilha e passo a passo, com modelos de documentos, para que você tenha condições de adequar os processos do seu provedor de acesso à internet em face da Lei Geral de Proteção de Dados Pessoais – LGPD.

Primeiro Passo: Entendendo a LGPD

Entender o propósito e os princípios básicos da LGPD é o primeiro passo para começar qualquer trabalho. Isto porque, a finalidade da coleta e tratamento de dados pelo provedor deve estar em conformidade com tais princípios, impactando, assim, na tomada de decisões quando do desenvolvimento e/ou implementação de novas tecnologias e novos serviços aos seus clientes.

I - Introdução

A LGPD se aplica ao provedor de acesso à internet? Sim!

A LGPD - Lei n.° 13.709/2018 - foi aprovada em 14 de Agosto de 2018 e entrará em vigor a partir de 15/08/2020. Muito influenciada pela lei europeia de proteção de dados (General Data Protection Rule, GDPR), a LGPD tem como propósito estabelecer princípios e critérios para o tratamento de dados pessoais, objetivando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa.

Além da própria LGPD, temos também a Lei n.° 13.853/2019, que criou a Autoridade Nacional de Proteção de Dados (ANPD) e estabeleceu sanções para os casos de descumprimento da LGPD. A regulamentação da ANPD ainda está pendente.

II - Principais conceitos da LGPD

Sempre que o provedor oferta ou comercializa produtos ou serviços, no Brasil, para uma pessoa física, ele está submetido às regras da LGPD para fins de tratamento de dados pessoais.

A partir disso, já tiramos a primeira informação importante: a LGPD não se aplica para o tratamento de dados de clientes ou potenciais clientes pessoas jurídicas.

O propósito da LGPD é tratar adequadamente os dados pessoais destes indivíduos.

E o que seria o "by design" e o "by default"?

A proteção de dados deve ser observada em todas as etapas de desenvolvimento dos produtos e/ou serviços e sempre na forma mais protetiva ao titular dos dados – ou seja, desde sua concepção (by design) e por padrão (by default) devem ser implementadas medidas de segurança, técnicas e administrativas que evitem o acesso não autorizado e de situações de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

E o que são dados pessoais?

Correspondem a toda informação relacionada à pessoa identificada - quando o dado estiver diretamente ligado a um indivíduo específico - ou identificável - quando, embora não vinculado diretamente, o dado permita descobrir a identidade de alguém a partir de sua análise, em conjunto com outras informações.

Alguns exemplos: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, e-mail, cookies e endereço IP.

Destaca-se: endereço IP é considerado dado pessoal.

A LGPD também criou uma categoria específica de dados pessoais chamada de “dados sensíveis”. Esses seriam aqueles de “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biométrica”.

Para os dados sensíveis, o consentimento deve ser destacado.
A regra é a mesma para o tratamento de dados de crianças e adolescentes, sendo que um dos pais ou responsável legal deve dar a autorização. O direito à informação aqui também é especial e exige mais cuidados. De acordo com o Estatuto da Criança e do Adolescente (ECA), considera-se “criança”, a pessoa com até 12 (doze) anos de idade incompletos, e “adolescente” aquela entre 12 (doze) e 18 (dezoito) anos.

III - Tratamento dos dados pessoais

Basicamente, tudo o que se faz com dados pessoais compõe o seu tratamento: coleta, classificação, armazenamento, transferência, envio para terceiros, eliminação e qualquer tipo de utilização que se faça deles.

Aqui tiramos outro conceito:

Você, provedor, é chamado de Controlador dos dados, pois cabe a você as decisões referentes ao tratamento de dados pessoais dos seus clientes e potenciais clientes, bem como seus empregados.

Todos aqueles que realizam o tratamento de dados pessoais em seu nome (desde funcionários até terceiros que recebem ou lidam de qualquer forma com esses dados) são chamados de Operador dos dados.

Exemplificando: quando o seu provedor envia uma lista de clientes inadimplentes para uma empresa terceirizada de cobrança, você está sujeito às regras de tratamento de dados da LGPD, enquanto Controlador, e a empresa de cobrança está sujeita às regras da LGPD na qualidade de Operador.

Quais são as hipóteses legais que permitem o tratamento de dados pessoais?

Como regra geral, para realizar o tratamento dos dados pessoais de seus clientes ou potenciais clientes, será necessário pedir o seu consentimento.

A nova lei se esforçou para que o consentimento seja real, isto é, feito de maneira consciente, livre e bem informada sobre a utilização dos dados e suas finalidades.

Então, o provedor deve se perguntar: em quais situações eu devo pedir esse consentimento e em quais situações a LGPD

apresenta uma exceção legal a essa exigência? Depende da situação.

Listamos, abaixo, os casos específicos em que se admite o tratamento de dados pessoais independente do consentimento prévio do titular, que interessam ao nosso mercado de provedores de acesso à internet:

1 - Para a execução de políticas públicas (pela Anatel e pelo MCTIC), bem como para a realização de estudos por órgãos de pesquisa (pelo IBGE, por exemplo). Atualmente, o SICI, o SGQ e as pesquisas feitas pelo IBGE não solicitam dados pessoais. Mas se um dia vierem a solicitar, o provedor está dispensado da necessidade de obtenção de consentimento do titular para fornecimento desses dados ao governo/instituição.

2 - Para cumprimento de obrigação legal ou regulatória do Controlador: é o caso do armazenamento dos registros de acesso a aplicações de internet pelo provedor de aplicações, como determinado pelo Marco Civil da Internet, bem como pelo armazenamento dos registros de conexão pelo provedor de acesso à internet, ou ainda o armazenamento de ligações telefônicas dos clientes para a central de atendimento do provedor.

3 – Para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual é parte o próprio titular: os provedores trabalham, em geral, com contratos de adesão com os clientes e devem inserir a previsão expressa de tratamento dos dados pessoais, visto tratar de condição essencial para a prestação do serviço. Esse cuidado no contrato de prestação de serviços é medida essencial para a LGPD, ainda mais se considerarmos o acesso e tratamento ao IP do cliente.

4 - Tratamento no exercício regular de direitos em processo judicial, administrativo ou arbitral: o tratamento de dados específico para o cumprimento de atividade de investigação policial ou cumprimento de ordem judicial para repressão de ilícito penal não se submetem a LGPD.

5 - Em caso de legítimo interesse do controlador ou de terceiro, desde que não se sobreponham aos direitos e liberdades fundamentais dos titulares dos dados.

Pode-se citar como exemplo, compartilhamento com empresas terceiras para fins de prevenção à fraude, marketing direto, proteção da integridade física do titular, dentre outras possibilidades. O legítimo interesse da empresa, nesse caso, atende uma finalidade que você já espera, estando dentro das suas expectativas e promovendo um serviço em seu benefício, ao mesmo tempo que serve de apoio para a atividade da empresa.

6-Tratamento para proteção de crédito: o tratamento de dados para que o provedor se certifique do crédito do cliente e da cobrança de uma dívida, por exemplo, é uma das possibilidades expressas da LGPD. Assim, por exemplo, o envio de dados de cobrança para uma empresa terceirizada não depende de consentimento prévio do cliente.

Alguns cuidados:

O desenvolvimento de novos serviços, que envolvam monitoramento de tráfego e perfil de acesso, devem ser muito bem avaliados com base na LGPD. Isso porque o perfil comportamental de um cliente pode ser, sim, considerado um dado pessoal, desde que a pessoa seja identificada.

IV - Princípios para o tratamento de dados

Todo o tratamento de dados pessoais deve observar alguns princípios. Destacaremos, inicialmente, três deles: finalidade, adequação e necessidade.

Os provedores têm o dever de apontar uma finalidade clara, justa e explícita antes de utilizar um dado, bem como devem adequar o tratamento a essa finalidade, devendo limitar-se ao que foi proposto ou ao que seja esperado pelo cliente.

Vamos exemplificar: imagine que seu provedor queira criar uma espécie de "score" para o cliente, ou seja, uma nota pessoal que objetiva prever como esse cliente se comportará no futuro em relação a suas obrigações financeiras ou em relação ao seu perfil de acesso ou de consumo de banda. Esse mesmo cliente, de acordo com os princípios da transparência e do livre acesso, tem o direito de saber as informações a respeito dessa nota: para que ela serve? Quais dados foram utilizados para compô-la? Por quanto tempo eles serão utilizados? Quem é o responsável pelo tratamento e como contatá-lo? E quais são os direitos do cliente? Caso seu provedor implemente esse tipo de tratamento de dados, avalie essas questões antes e faça constar de seu Relatório DPIA e Política de Privacidade, abaixo apresentados.

Também, o cliente ou potencial cliente tem direito ao acesso fácil, claro e gratuito sobre todas essas informações e dados pessoais. O livre acesso é também uma forma do titular garantir que seus dados permaneçam íntegros e não adulterados, ajudando a assegurar outro princípio da lei: a não discriminação ilícita ou abusiva das pessoas como resultado do tratamento de dados.

Para impedir o tratamento discriminatório, é essencial o respeito a outro princípio da lei, o da qualidade dos dados. Os dados devem ser precisos, claros, relevantes e atualizados, minimizando, assim, a existência de erros e abusos.

Caso o cliente entre em contato solicitando confirmação e acesso aos dados, a empresa poderá responder imediatamente de forma

simplificada ou em até 15 dias com informações mais completas ou complexas.

Por isso, é importante que os dados sejam bem cuidados, sendo aqui essenciais os três últimos princípios da Lei: segurança dos dados, prevenção de acidentes ou atividades ilícitas e responsabilização e prestação de contas.

Além desses cuidados acima, a LGPD traz uma alternativa técnica para tratamento de dados, que facilita a vida do provedor: o processo de anonimização, que desassocia o dado da pessoa titular.

Há várias formas para realizar esta desassociação, como a eliminação de qualquer informação de identificação pessoal (nome, RG, CPF, etc.) e a encriptação, capaz de codificar as informações pessoais, transformando-as em dados ilegíveis a todos que não possuírem a chave de encriptação.

É, assim, uma ferramenta muito importante, já que permite o tratamento de dados com menos riscos. Por isso, a LGPD prevê que seja feita a anonimização, sempre que possível, especialmente em casos de utilização para políticas públicas ou tratamento de dados sensíveis.

Use e abuse das técnicas de anonimização, de forma consistente. Isso pode ser a chave de uma defesa futura de descumprimento da LGPD.

Esta desvinculação, inclusive, faz com que o dado anonimizado não seja considerado um dado pessoal, tendo em vista que não se refere a ninguém identificável. Mas ainda há uma polêmica envolvendo a possibilidade de reversão da anonimização. Por conta disso, a Lei abre uma exceção a esta regra: se o dado for novamente associado àquele titular, então ele volta a ser considerado um dado pessoal.

Outro é o cenário dos dados pseudoanonimizados, que são sim considerados dados pessoais e correspondem àqueles que permitem a associação a um indivíduo a partir de informações mantidas pelo controlador em um ambiente (banco de dados) restrito e seguro do Controlador.

V - Outros direitos dos titulares de dados pessoais

Além do que já foi exposto acima, o titular dos dados pessoais possui os seguintes direitos:

- Retificação dos dados, para corrigir dados incompletos, inexatos ou desatualizados que lhes digam respeito.

- Restrição de tratamento: os titulares possuem o direito de restringir o tratamento de dados pessoais, por meio da recusa em fornecer o consentimento.

- Cancelamento ou Exclusão de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD ou cujo consentimento do Usuário for retirado.

- Portabilidade: o titular tem o direito de receber todos os seus dados pessoais que tenham sido fornecidos a um controlador, inclusive em formato eletrônico e interoperável, a fim de que estes sejam transmitidos a outro fornecedor de serviço ou produto, de escolha do titular. Esse direito ainda depende de regulamentação por parte da Autoridade Nacional de Proteção de Dados.

- Revogação de Consentimento: o titular dos dados pode revogar o consentimento para tratamento de seus dados pessoais a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado. O provedor poderá continuar o tratamento dos dados pessoais obtidos, mediante consentimento, anteriormente ao pedido de revogação, até que a finalidade do tratamento seja alcançada ou nas demais hipóteses previstas em lei.

- Oposição: o titular dos dados tem o direito de se opor a quaisquer tratamentos e informações que não estejam em conformidade com a lei, bem como a decisões automatizadas que afetem seus interesses, como decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (profiling).

- Explicação: o titular dos dados tem direito a receber informações claras e adequadas a respeito dos critérios e dos procedimentos

utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais.

A LGPD estabelece que os direitos previstos aqui serão exercidos mediante requerimento expresso do titular ou de representante legal, iniciando o prazo para resposta do Controlador dos dados. Diante disso, sugerimos que o provedor estabeleça um formulário padrão, que contenha uma identificação de documento, a identificação do cliente, seu pedido e a data. A resposta do provedor deve vir acompanhada do número de protocolo aberto com essa finalidade de tratamento. Sugerimos que a resposta seja enviada via e-mail ao cliente, mas não há previsão expressa na lei sobre esse formalismo.

VI - Conheça alguns casos de descumprimento da LGPD e responsabilização

Achamos relevante que o provedor conheça dois episódios considerados pelas autoridades brasileiras de descumprimento de princípios refletidos na LGPD:

Em 2010, a empresa Oi S.A. começou a mapear hábitos de acesso à internet dos usuários do serviço Velox, sem consentimento. Batizado de Navegador, o programa utilizado para coleta de dados traçava perfis de consumo, que eram comercializados para realização de publicidade direcionada.

Diante disso, o Departamento de Proteção e Defesa do Consumidor (DPDC) instaurou processo administrativo para apurar as irregularidades cometidas e concluiu, em 2014, que a coleta e compartilhamento de dados pessoais sem consentimento informado e expresso dos titulares importavam em violação do princípio da autodeterminação informativa, correspondente ao direito essencial de controlar e proteger seus próprios dados pessoais. A empresa foi multada em R$3,5 milhões.

Outro caso aconteceu com a Vivo S.A. O Ministério Público do Distrito Federal e Territórios, por meio da Unidade Especial de Proteção de Dados Pessoais e Inteligência Artificial (Espec), conseguiu na Justiça a suspensão da comercialização do produto Mídia Geolocalizada da plataforma Vivo Ads, além de ordem judicial obrigando a empresa a elaborar e a entregar ao Poder Judiciário Relatório de Impacto à Proteção de Dados Pessoais (DPIA, abaixo comentado).

A operadora foi acusada de vender para empresas o produto Vivo Ads, que consiste no tratamento ilegal do perfil, da geolocalização, do histórico de navegação e dos lugares frequentados pelos clientes da Vivo. Os dados colhidos e tratados em tempo real eram usados para traçar o comportamento das pessoas e direcionar o marketing, conforme interesse de quem demandava o serviço.

As empresas interessadas identificavam quais os locais físicos que desejavam impactar em sua campanha e o tipo de ação do consumidor

capaz de ativar a publicidade: entrada, saída ou permanência por determinado período em determinado local ou região. Assim, toda vez que um cliente interagia no local indicado e na forma especificada pelo anunciante, a Vivo disparava uma mensagem com anúncio disponível na plataforma. O produto permitia, assim, que consumidores recebessem ofertas e promoções de estabelecimentos comerciais próximos.

O processo ainda está em andamento.

Quais as sanções por descumprimento da LGPD?

Esclarecemos que a LGPD estabelece diversas sanções administrativas a serem aplicadas pela Autoridade Nacional aos agentes de tratamento (controlador e/ou operador) que infringirem as normas previstas na Lei: desde a advertência, com indicação de prazo para adoção de medidas corretivas, até multa simples de até 2% (dois por cento) do faturamento da empresa, por infração. Também estabelece multa diária, obrigação de dar publicidade à infração, bloqueio dos dados pessoais ou eliminação desses a que se refere a infração.

Outros pontos sancionatórios recém confirmados pelo Congresso Nacional, após a derrubada de vetos do Executivo, foi a possibilidade de suspensão do exercício da atividade de tratamento dos dados pessoais e a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

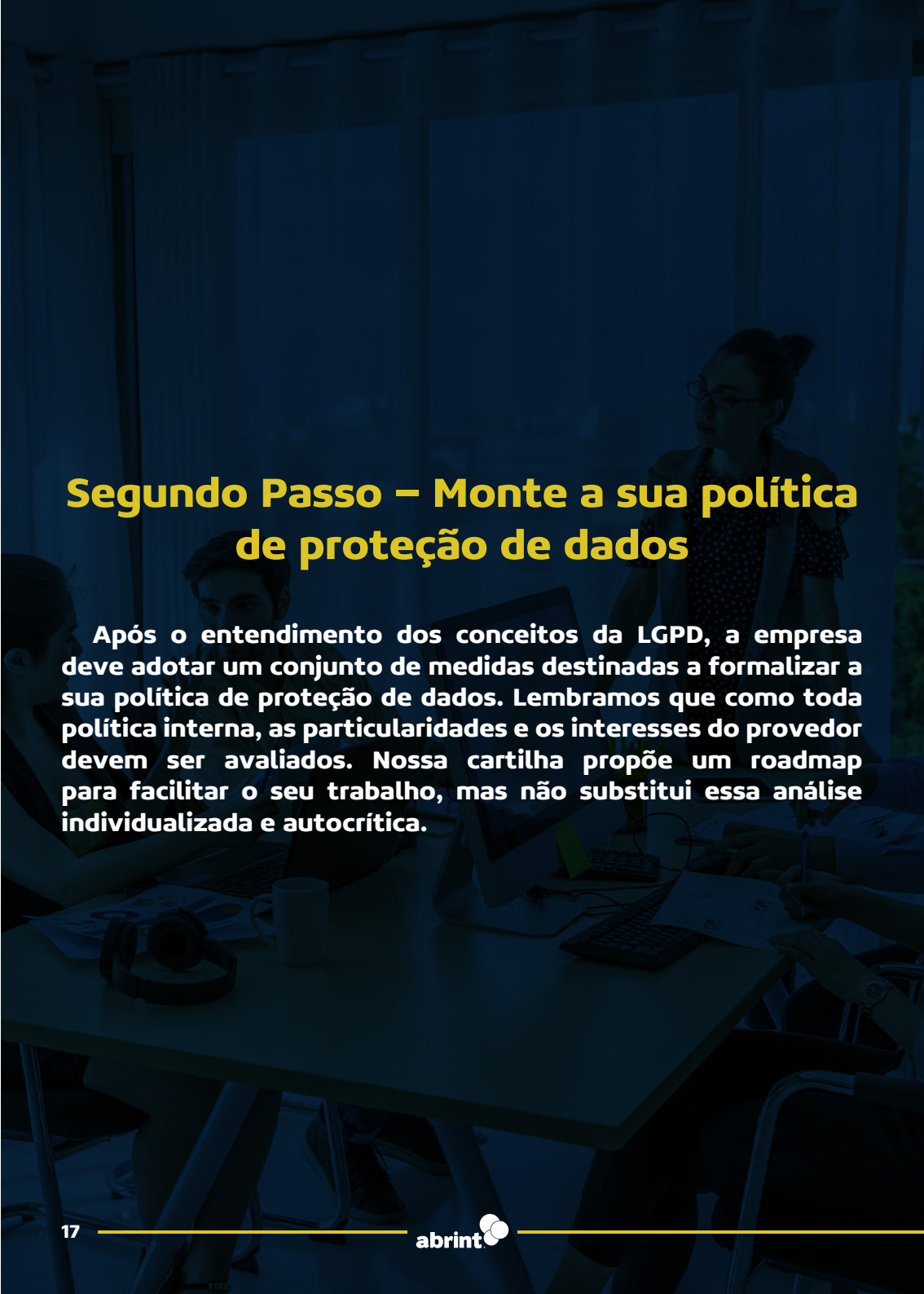
O Congresso também confirmou que a aplicação das sanções independe do fato do Controlador estar submetido à regulação/controle de outro órgão, distinto da própria ANPD. Esse aspecto é de suma relevância para as atividades de telecomunicações, reguladas pela Anatel, a carga dos provedores.

A aplicação das sanções considera, dentre outros elementos, a adoção pelo controlador ou operador de mecanismos e procedimentos para minimizar os danos, bem como a adoção de políticas de boas práticas e governança. Assim, não há dúvidas de que o melhor caminho é entender e se preparar.

Uma empresa não será responsabilizada judicialmente apenas em casos que comprovem: que na verdade não realizou aquele tratamento de dados; que não houve violação à legislação de proteção de dados - ou seja, se comprovar que cumpriu com todos os deveres de segurança, utilizando todas as medidas técnicas possíveis; ou que o dano foi causado por culpa exclusiva do titular dos dados ou de terceiro.

Sob o aspecto da responsabilização, a LGPD estabelece obrigações gerais e específicas para ambos os agentes de tratamento, controlador e operador, de forma que ambos podem ser, inclusive, responsabilizados solidariamente.

Via de regra, é de responsabilidade do Controlador: comprovar que o consentimento foi obtido, bem como informar ao Operador eventual pedido de revogação de consentimento e/ou eliminação de dados pelo respectivo titular, a fim de que este suspenda o tratamento ou providencie a anonimização e/ou o apagamento dos dados. Já com relação ao Operador, é de sua responsabilidade: seguir todas as medidas técnicas e administrativas de tratamento instruídas pelo Controlador, sob pena de responder solidariamente pelos danos causados aos titulares.



Segundo Passo – Monte a sua política de proteção de dados

Após o entendimento dos conceitos da LGPD, a empresa deve adotar um conjunto de medidas destinadas a formalizar a sua política de proteção de dados. Lembramos que como toda política interna, as particularidades e os interesses do provedor devem ser avaliados. Nossa cartilha propõe um roadmap para facilitar o seu trabalho, mas não substitui essa análise individualizada e autocrítica.

Sugerimos que o provedor identifique alguém de sua estrutura para liderar esse processo, capaz de interagir com os demais setores da empresa e com atribuições claras de implementar uma política de privacidade de proteção de dados. Se houver possibilidade dessa pessoa contar com uma equipe multidisciplinar, formada pelos gestores dos setores de TI, Operações, Comercial, Financeiro e RH (assim denominados usualmente), melhor ainda será o resultado.

Comece o trabalho estruturando um mapa de tratamento de dados, chamado Relatório de impacto à proteção de dados pessoais.

Basicamente, esse documento corresponde ao conceito do "DPIA", a sigla para Data Protection Impact Assessment, uma metodologia amplamente adotada pela legislação europeia de proteção de dados pessoais, que foi incorporada pela nossa LGPD sob o nome de "Relatório de impacto à proteção de dados pessoais". Consiste em uma documentação que descreve os processos de coleta e tratamento de dados pessoais, capazes de gerar algum risco aos direitos dos titulares, além das medidas e mecanismos empregados para mitigar esses riscos.

Esse relatório pode ser estruturado a partir de um excel mesmo, se você preferir. A construção do relatório parte do detalhamento de todos os processos de coleta e tratamento pelos quais os dados pessoais passam durante o ciclo de vida no seu provedor, desde o primeiro contato com tais dados pessoais, até a sua exclusão das bases de dados.

O relatório deve mostrar quais são os momentos de coleta e tratamento dos dados, os setores do provedor e as pessoas (empregados e terceirizados)/empresas terceiras envolvidas, as bases legais e a finalidade da coleta ou tratamento, bem como as medidas de segurança adotadas nesse processo. Aquela pergunta essencial - preciso colocar um check box de consentimento prévio? – será respondida aqui, nesse "mapa", a cada processo de coleta e tratamento de dados identificado no provedor.

Exemplificamos: Quando o setor de RH recebe um currículo, nesse relatório deve constar, minimamente:

- Setor envolvido: RH

- Pessoas envolvidas: analista RH, gestor da área da vaga

- Terceiros envolvidos: escritório contábil ou escritório de banco de talentos.

- Processos envolvidos: a)recebimento do currículo via e-mail; b)processo de seleção; c)processo de contratação; d)eSocial

- Base legal / finalidade: contratação e levantamento de informações para eocial.

- Local de armazenamento dos dados: erp xxx.

- Prazo de armazenamento dos dados: depende muito da situação e do conservadorismo da empresa. Para questões estritamente trabalhistas, sugerimos mínimo de 5 anos.

- Há contrato/documento envolvido? Sim: formulário de teste admissional, contrato de trabalho e manual de boas vindas do empregado.

- Medidas de segurança: acesso restrito de categoria de usuário, criptografia, etc.

- Consentimento prévio: sim - Inserção de cláusula em contrato de trabalho de empregado e inserção de checkbox em formulário de entrevista/teste admissional.

Esclarecendo: aqui temos um processo específico, que foi identificado e mapeado e que estabelecemos as medidas de segurança e a necessidade de consentimento prévio.

Nem todos os casos de coleta e tratamento de dados exigem essa última linha de consentimento prévio.

Outro exemplo: provedor coleta dados de clientes para ativação de serviço; provedor trata de inadimplência de cliente e envia arquivos de cobrança para empresa terceira; provedor oferece serviço de marketing direcionado ao IP.

Os processos acima exemplificados envolvem coleta e tratamento de dados pessoais. O relatório de impacto deverá esmiuçar todo o ciclo desses processos e envolvidos, de maneira muito semelhante ao exemplo do RH. Em caso de falha, aciona-se os responsáveis mapeados (internos ou externos ao provedor, tal como um fornecedor de software ou serviço) e adota-se as medidas de segurança mapeadas.

Nos dois primeiros casos, as situações legais de tratamento de dados da LGPD acima comentadas - para execução de contrato e para tratamento de crédito, respectivamente - dispensam o consentimento prévio do cliente. Uma simples cláusula integrante do contrato de adesão já é suficiente.

Já no terceiro caso – profiling – não se trata de tratado de dado relacionado diretamente à finalidade do contrato de serviços de banda larga. Nesse caso, exige sim um checkbox de consentimento prévio. Pode ser inserido no formulário de contratação do serviço.

Outro aspecto essencial para ser mapeado é o grau de confiabilidade dos próprios sistemas utilizados pelo provedor ou contratados de terceiros.

A forma de remessa de arquivos do provedor, que eventualmente ocorra em um ou outro processo, deve ser objeto de adoção prévia de medida de segurança, exemplo: o SFTP, ou protocolo de transferência de arquivos SSH, é a implementação segura mais popular do FTP.

A descrição detalhada do ciclo de vida dos dados pessoais no seu provedor, associada à consulta e a colaboração com os agentes envolvidos, permite identificar os pontos de fragilidade da operação, que podem representar algum risco aos direitos dos titulares dos dados. Esse mapeamento de processo busca antecipar a avaliação desses riscos, a partir da qual são identificadas as medidas necessárias para a sua contenção, que devem ser implementadas e testadas pelo provedor.

Portanto, embora a antecipação da produção desse relatório não seja obrigatória pela LGPD, tal prática é bastante recomendável.

Em caso de eventual auditoria ou processo administrativo perante a Autoridade Nacional - ANPD, essa documentação poderá servir como base para demonstrar a boa-fé do provedor, a diligência e o comprometimento da empresa em termos de governança, conformidade com a legislação e preocupação com a segurança e sigilo dos dados pessoais dos titulares e, por conseguinte, atenuar eventual sanção administrativa.

Como o relatório de impacto à proteção de dados pessoais contém informações confidenciais do provedor, inclusive relacionadas à sua forma de organização, não se trata de um documento adequado para se dar publicidade, mas tão somente para que o provedor guarde e controle tais processos, internamente.

Dessa forma, entendemos que o processo de implantação da adequação à LGPD deve ser comunicado aos colaboradores de uma maneira geral, seguindo os conceitos e princípios básicos da LGPD da primeira parte do trabalho. Não recomendamos a veiculação de detalhes do processo, mas apenas aquilo que seja realmente relevante e sempre com foco conceitual.

Tendo sido realizado um bom trabalho de mapeamento dos processos que envolvem coleta e tratamento de dados pessoais (que podem envolver dados pessoais de clientes, potenciais cliente, colaboradores terceirizados e de funcionários), naturalmente (assim se espera) que cada contrato e termo vigente (relacionado à tais processos) seja revisado.

Retomando o exemplo acima do setor de RH do provedor, tendo sido identificados os três documentos que participam, de alguma forma, aos processos mapeados (formulário de teste admissional, contrato de trabalho e manual de boas-vindas), faça a revisão desses para ver se o consentimento indicado no mapa é ou não suficiente.

Dessa forma, essa é a etapa de adequar seus contratos e termos a LGPD, verificando se há cláusulas específicas sobre proteção de dados pessoais, consentimento expresso, confidencialidade e responsabilidades civis, criminais e/ou administrativas concernentes. O mesmo se aplica para Políticas, Normas e Processos Internos relacionados à Segurança da Informação, site do provedor, plano de cargos e salários, acordo coletivo, etc.

Recordemos um pouco a primeira etapa dessa cartilha: nem tudo exige consentimento do cliente, pois pode se tratar de caso legal de tratamento de dados decorrente do legítimo interesse do Controlador. Exemplo: não excluir dados financeiros de um contrato pois há legítimo interesse, decorrente de contrato firmado, de se cobrar um

cliente inadimplente, mesmo após o contrato estar cancelado e o serviço desativado.

De maneira bastante prática, teremos:

Contrato de prestação de serviço para clientes: o seu provedor deve avaliar o tipo de serviço prestado e os dados pessoais relacionados. Exemplo: um contrato de prestação de serviços de comunicação multimídia com cliente residencial envolve dados distintos de um contrato de prestação de serviços de telefonia fixa ou de armazenamento em cloud.

Pensando no contrato de prestação de serviços de comunicação multimídia, veja a proposta do **Anexo I.**

Agora, com relação aos contratos de licença de uso e gestão de software com fornecedor, que colete e trate dados pessoais, verifique o modelo do **Anexo II** sugerido.

Já com relação à política de privacidade de acesso ao site do provedor, avalie o **Anexo III.**

Com relação aos contratos de trabalho com os colaboradores, veja a solução de cláusula do **Anexo IV.**

Alguns provedores talvez trabalhem com ações de marketing direto para aquisição de serviços. Cuidados extras devem ser tomados a partir da configuração de protocolos e processos para opt-in e opt-out. Reforçamos as recomendações acima sobre score e profiling.

Terceiro Passo– LGPD na rotina do provedor

Resolvidas as etapas anteriores, o provedor deve criar um programa de compliance que vai acompanhar e atestar o seguimento às diretrizes e medidas de segurança adotadas naquele mapa - DPIA, de forma contínua, com previsão, inclusive, de revisão periódica.

O programa de compliance deve documentar todas as atividades envolvidas no tratamento de dados pessoais e demonstrar todos os esforços para que estejam em conformidade com a LGPD, integrando os princípios da prevenção, segurança, transparência e prestação de contas (accountability) que fundamentam a LGPD.

Esse programa pressupõe a nomeação, pelo provedor, de um "Encarregado pelo Tratamento de Dados Pessoais", conhecido como Data Protection Officer (DPO). Essa nomeação deve ser divulgada de forma clara e objetiva, de preferência no site do próprio provedor, com a identidade e as informações de contato do encarregado.

A Autoridade Nacional poderá estabelecer normas específicas sobre as funções e eventuais hipóteses de dispensa da necessidade de indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

A redação original da LGPD previa expressamente que a função fosse exercida por pessoa física. A MP 869 alterou a redação, ampliando a possibilidade de atuação inclusive por pessoas jurídicas e terceirizadas, semelhante ao que se estabeleceu na Europa.

Também, caso haja um incidente de tratamento de dados pessoais, que possa acarretar risco ou dano relevante aos titulares, seguindo os princípios de transparência e informação, é de responsabilidade do provedor comunicar o fato à Autoridade Nacional e ao titular desses dados.

Outras informações

Caso queiram conhecer todo o caminho do processo legislativo da LGPD, sugerimos acessar o site https://www.portaldaprivacidade.com.br/1anolgpd

Para saber algumas das soluções de sistemas e fornecedores voltados especificamente para o tratamento profissional de dados, utilizados por empresas de grande porte, acessem:

https://drive.google.com/file/d/16euZfeqzsMDe-hJhfnoHrghu88rcDOyN/view

Atenção: os modelos sugerido nas próximas páginas são modelos conceituais. Você deve adaptá-los à sua realidade e aos seus processos, sob pena do trabalho ser em vão.

Anexo I: Contrato de prestação de serviços

"**1.** Nos termos do Regulamento dos Serviços de Comunicação Multimídia, aprovado pela Resolução ANATEL 614/2013, bem como de acordo com a Lei n.º 12.965/2014 (Marco Civil da Internet), a Contratada deverá manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo de 01 (um) ano.

2. A Contratada observará o dever de zelar estritamente pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade quanto aos dados cadastrais e informações do Cliente, sobretudo no que se refere aos registros de conexão armazenados, empregando para tanto todos os meios e tecnologias necessárias para assegurar o direito do Cliente.

3. A CONTRATADA apenas tornará disponíveis os dados cadastrais e os registros de conexão, incorrendo em suspensão de sigilo de telecomunicações, quando solicitado formalmente pela autoridade judiciária ou outra legalmente investida desses poderes, e quando taxativamente determinada a apresentação de informações relativas ao CLIENTE.

4. A adesão ao presente Contrato importa na ciência e na concordância do Cliente de que o uso de seus dados pessoais (nome, telefone, e-mail e empresa vinculada) pela Contratada é condição necessária para o fornecimento dos serviços estabelecidos via contrato de adesão, nos termos do §3°, do art. 9° da Lei 13.709/18. O mesmo se aplica para o endereço IP do cliente, especialmente por se tratar de gestão de dado pessoal decorrente de cumprimento de obrigação legal e regulatória."

Anexo II: Acordo voltado para terceiros, na qualidade de operadores do tratamento de dados

TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS E INFORMAÇÕES

Pelo presente instrumento, a _____, inscrita no CNPJ sob o n.º _____, com sede na _____, e de outro lado, a empresa _____ _____, pessoa jurídica do tipo _____, CNPJ nº_____, com sede em _____, neste ato representada, conforme poderes especialmente conferidos, por _____, na qualidade de _____ CPF nº _____, Identidade nº _____, expedida por _____, doravante denominado Parte Receptora, têm entre si ajustado o que se segue:

1. DO OBJETO

1.1. Este termo de confidencialidade pretende dar proteção adequada e suficiente às Informações Confidenciais e dados pessoais transmitidas pela xx para a Receptora, próprias ou de terceiros, em função da celebração de contrato de prestação de serviços cujo objeto é xxxxx.

2. DAS INFORMAÇÕES CONFIDENCIAIS E OUTROS CONCEITOS

2.1. Para os fins deste acordo, serão consideradas confidenciais todas as informações, transmitidas por meios:

I- Escritos;

II- Eletrônicos;

III- Verbais e/ou visual;

IV- Pelo início do acesso às Informações, seja ou não contidas em um banco de dados, bem como acesso remoto ou através do envio de arquivos.

2.1.1. Toda e qualquer Informação referente à dados pessoais de clientes, potenciais ou não, da xxxxx, bem como senhas, endereços IP, endereços de MAC, configurações de rede, roteadores, localização

de estações de rádio transmissão e/ou Caixas de Transmissão Óptica, políticas comerciais (tais como política de preços, dados financeiros, estatísticos, dados de funcionários, contratos, estratégias de expansão da empresa, parcerias, dentre outras) e dados relativos à forma e infraestrutura utilizada para a prestação dos serviços serão consideradas confidenciais.

2.1.2. Em caso de dúvida sobre a confidencialidade de determinada informação, a Parte Receptora deverá mantê-la em absoluto sigilo, até que a xxxxx se manifeste expressamente a respeito.

2.1.3. Não há hipótese legal que admita situação de tratamento de dados pessoais e informações confidenciais de propriedade da xxx pela Parte Receptora, sendo vedada qualquer espécie de avaliação, coleta, estudo ou trabalho sobre tais dados e informações, bem como uso pela Receptora para balizar serviços ou produtos. Não se aplica à Parte Receptora as hipóteses legais previstas no art. 7° da Lei 13.709/2018 e o descumprimento dessa cláusula importará em multa contratual abaixo prevista.

2.1.4. A Parte Receptora não transferirá nem de outra forma divulgará Dados e Informações da xx, nem permitirá o processamento deles por seus Representantes ou quaisquer Terceiros, sob pena de descumprimento das regras estabelecidas nesse Acordo.

3. DA SEGURANÇA E DAS OBRIGAÇÕES

3.1. A Parte Receptora se responsabiliza integralmente por toda e qualquer atividade que possa, diretamente ou não, expor os dados e informações a vazamentos ao acesso não autorizado.

3.2. A Parte Receptora se responsabiliza pela proteção de seu banco de dados e ambientes operacionais contra acessos internos e externos, e contra explorações de bases de dados.

3.3. A Parte Receptora se responsabiliza pela prevenção avançada contra ameaças e ataques a nível de rede.

3.4. A Parte Receptora se responsabiliza pela proteção contra ataques em ambientes de nuvens privadas e públicas.

3.5. Em caso de qualquer falha na segurança das informações confidenciais e dados pessoais, a Parte Receptora deverá comunicar imediatamente a xx. A pronta comunicação da Parte Receptora não

exclui, entretanto, a sua responsabilização pelo descumprimento na proteção efetiva dos dados e informações.

3.6. A Parte Receptora obriga-se a:

a) Não divulgar ou disseminar as informações da xx, para qualquer outra pessoa, física ou jurídica, salvo mediante autorização prévia e por escrito da xx.

b) Utilizar as Informações da xx para os fins a que exclusivamente se destina, nos termos da divulgação, durante o exercício da prestação de serviços, devendo realizar a devolução integral de todo e qualquer dado ou informação ao término do contrato.

3.7. A Parte Receptora não poderá instalar ou testar qualquer espécie de script ou redirecionamento de arquivos não autorizado expressamente e por escrito pela empresa, sob pena disso ser compreendido como descumprimento contratual e quebra de sigilo de dados.

3.8. Caso Parte Receptora seja obrigada por determinação legal a fornecer as Informações à autoridade competente, deverá informar previamente a xx para que esta tome as medidas que julgar cabíveis. A Parte Receptora não responderá a tal solicitação, determinação, consulta ou reclamação, a menos que seja instruído por escrito pela xx.

3.9. A Parte Receptora terá e manterá processos físicos, organizacionais e técnicos, padrões de segurança, diretrizes, controles e procedimentos apropriados e padronizados para proteger-se contra quaisquer Violações de Dados. A Parte Receptora é exclusivamente responsável pela implantação de todas as medidas de segurança e controle sobre vulnerabilidades, gerenciamento de dados, políticas de Controle de acesso e gerenciamento de identidades, políticas de conscientização e treinamento. A implantação desses cuidados não exime a Parte Receptora de qualquer quebra de sigilo de dados pessoais e informações confidenciais.

3.10. Fica estabelecido que todo o conteúdo existente nas máquinas e computadores alocados na xx ou em ambiente cloud contratado para a prestação dos serviços são de propriedade exclusiva da xx. A Parte Receptora não poderá efetuar qualquer cópia ou backup deste conteúdo para uso próprio ou de terceiros, salvo mediante prévia e expressa autorização da xx.

3.11. A xx se reserva o direito de apagar arquivos e programas, formatar ou dar fim diverso à máquina ou bando de dados de sua propriedade.

4. DAS PENALIDADES

4.1. O descumprimento das obrigações previstas acima a apuração dos danos diretos e indiretos sofridos pela xx, bem como lucros cessantes referentes aos titulares dos dados pessoais.

4.2. Sem exclusão das demais formas de descumprimento contratual, eventual acesso não autorizado da rede da xx feito pela Parte Receptora ou por terceiro relacionado, com potencialidade de causar dano à estrutura e configuração da rede ou à base de dados da xx, configura crime de dano e se submete ao disposto na cláusula acima.

5. DO PERÍODO DE CONFIDENCIALIDADE E DEMAIS DISPOSIÇÕES CONTRATUAIS

5.1. As Informações permanecem confidenciais por prazo indeterminado.

5.2. Quando da rescisão do Contrato de Prestação de Serviços ou mediante solicitação por escrito da xx, o que ocorrer primeiro, a Parte receptora cessará imediatamente, e garantirá que seus Subcontratados cessem imediatamente, todo e qualquer uso de tais Dados Pessoais e Informações, devolvendo-os xx ou, mediante instruções da xx, descartando-os, destruindo-os ou tornando-os anônimos de forma permanente.

5.3. Eventual rescisão da prestação de Serviços não exime a Parte Receptora das obrigações e penalidades previstas neste Contrato.

5.4. O presente Termo tem natureza irrevogável e irretratável e o seu não cumprimento acarretará todos os efeitos de ordem penal, civil e administrativa contra seus transgressores.

5.5. Para dirimir quaisquer dúvidas oriundas do presente Termo, fica eleito o foro da Comarca de xx/xx.

E por estarem justas e acordadas, as PARTES assinam este instrumento em 02 (duas) vias de idêntico conteúdo e forma.

xxx, dia de Mês de 2019.

_____ _____

Parte Receptora xx

Anexo III: Política de Privacidade (inclusive para site)

Introdução:

Este site e essa Política de Privacidade são de propriedade da xxxx a xxxx, em conformidade com a Lei Geral de Proteção de Dados, estabeleceu uma normativa interna de proteção de dados através de medidas concretas de mapeamento do fluxo de dados, contratos específicos com fornecedores, termo de consentimento firmado com empregados e colaboradores e adequação dos seus Contratos de Prestação de Serviços.

O propósito dessa Política de Privacidade é dar transparência à forma como se dá a coleta e o tratamento dos dados fornecidos pelos clientes, seja ao acessar o site da xxx, seja ao contratar nossos serviços.

Buscamos garantir que os dados de caráter pessoal sejam tratados de forma adequada e sigam as diretrizes estabelecidas na legislação nacional.

As Premissas da xxx:

1 - A coleta e o tratamento de dados observa o princípio fundamental de privacidade dos clientes, seja através da garantia da confidencialidade desses dados, seja através de técnicas de anonimização e pseudoanonimização.

2 - A xxxx garante a aplicação de controles de segurança e implantação de níveis de acesso diferenciados aos sistemas, a fim de mitigar o risco de vazamento de dados e demais ameaças à segurança das informações.

Sobre a coleta e uso de Informações pessoais:

1 - A coleta de dados pessoais se dá para fins de execução de contrato de prestação de serviços, bem como para fins de adequação à regulação dos serviços de telecomunicações.

2- A adoção de medidas protetivas à privacidade e segurança dos dados se dá desde a concepção do serviço (privacy by design). A xxx entende “tratamento de dados” como toda e qualquer 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.

3- A coleta dos dados sempre observa a autorização do cliente (OPT-IN) através de formulários padrão e preenchidos pelo próprio cliente através do uso do site.

4- As informações podem ser utilizadas pela xxx para o envio de ofertas de serviços e a fim de proporcionar uma melhor experiência do cliente e satisfação com relação aos nossos serviços.

5- As informações são coletadas no momento do cadastro da venda, seja por parceiro de vendas, seja diretamente na central de Atendimento, ou ao acessar nosso site.

6- A xxx poderá fazer uso de cookies para confirmar sua identidade, personalizar seu acesso e acompanhar a utilização de nosso site. Os cookies são informações enviadas pelo servidor do site xxxx ao computador do usuário para identificação. Com isso, podemos identificar quantas pessoas visitam o site, como um grupo de usuários o utiliza e quais são as páginas preferidas pelo público. A informação não nos permite identificar o usuário, tampouco seu endereço. Ela apenas permite que, a partir de tendências de navegação, aprimoremos a navegabilidade do site. A aceitação dos cookies pode ser livremente alterada na configuração de seu navegador de internet.

7- Em nosso site podem existir links que levam a outras páginas que ficam fora de nosso site/servidor. Esses links são disponibilizados apenas para sua conveniência. Não nos responsabilizamos pelo conteúdo ou material que possa ser encontrado nesses sites. As operações e o conteúdo desses sites estão fora de nosso controle e, a utilização desses sites, dos produtos e serviços anunciados ou

vendidos nesses sites é de total responsabilidade do usuário.

8 - Não nos responsabilizamos por qualquer prejuízo, direto ou indireto, que possa surgir em virtude da utilização de nosso site ou de qualquer outro site que esteja disponível por meio de link disponível em nosso site.

9 - Todas as informações são tratadas em sistemas internos da xxxx, dotados de controle de acesso e treinamento adequado para os usuários.

Do Tratamento dos Dados:

1 - Em alguns casos, conforme política de classificação de dados, a informação pode ser compartilhada com empresas parceiras e fornecedores, sujeitos às mesmas regras de confidencialidade, privacidade e controles de segurança, estabelecidas através de acordos de confidencialidade assinados entre as Partes.

2 - A xx está comprometida com a transparência no uso das informações dos clientes, sempre em busca de adequação da sua oferta de serviços contratados e da experiência diferenciada do cliente.

3 - A xx coleta:

a) Dados pessoais: Nome, endereço, RG, CPF, telefone, e-mail, data de nascimento (quando relevante). Não solicitamos através do site ou através de e-mail quaisquer informações bancárias ou relativas a qualquer meio de pagamento. Caso o cliente opte pelo pagamento dos serviços através de cartão de crédito, o setor financeiro da empresa, através do telefone da central de atendimento, entrará em contato para coleta de dados e a ligação poderá ser gravada.

b) Endereço IP: A xxx fará a coleta de informações de endereços de IP e logs de acesso (dados de conexão, data e hora) utilizado pelo terminal do cliente para o envio e recebimento de pacotes de dados, nos termos exigidos pelo Marco Civil da Internet. A xxx é proprietária do endereço IP alocado para o cliente na oferta de serviços e o cancelamento do contrato implicará na restituição desse endereço à xxx.

c) Análise de Crédito: A xx realiza a análise de crédito do cliente para a venda de serviços, junto ao Serasa, ao SCPC e Sistema de Cadastro Positivo. Tais informações podem ser excluídas de nossa base de dados através de pedido específico encaminhado pelo Cliente, conforme estabelecido abaixo.

4 - A xxx poderá, a partir de política de classificação de dados, fazer uso de técnicas de anonimização de dados (dados pessoais relativos a um titular que não possa ser identificado) e pseudoanonimização (com uso de elementos de identificação encriptados), a fim de permitir pesquisas, análises de tráfego e otimização de desempenho de rede e oferta de serviços.

5 - A política interna de segurança das informações baseia-se em adoção de técnicas de criptografia para dados financeiros, permissões de acesso diferenciadas, rotinas de treinamento de uso de sistemas, manutenção de programas de gerenciamento de vulnerabilidades e acompanhamento e testes regulares de rede, gerenciamento do consentimento e do ciclo de vida dos dados, além da atualização anual de DPIA e elaboração de plano de ação e reporte em caso de incidentes.

Das exceções:

1 - Exceções de compartilhamento das suas informações são aplicáveis em casos de solicitações judiciais feita pelos órgãos competentes, que serão disponibilizadas sem conhecimento do cliente, conforme abaixo fundamentado:

1.1. O Marco Civil da Internet, em seu artigo 10, diferencia as hipóteses nas quais autoridades públicas podem ter acesso a dados cadastrais e a registros de conexão.

1.2. Os registros de conexão somente podem ser disponibilizados para o requisitante se a entrega for autorizada por ordem judicial (art. 10, §1º). Já os dados cadastrais podem ser disponibilizados diretamente para autoridades administrativas, sem necessidade de ordem judicial, se e quando possuem competência legal para a requisição (art. 10, § 3º). Além disso, o art. 11 do Decreto no 8.771/2016, que regulamenta

alguns aspectos do Marco Civil da Internet, determina que a autoridade administrativa deve indicar no pedido o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

1.3 Atualmente, autoridades policiais e do Ministério Público possuem autoridade para requisição de dados cadastrais no âmbito de aplicação da Lei das Organizações Criminosas e da Lei dos Crimes de Lavagem de Dinheiro. Nesse sentido, a xxx adota a interpretação mais protetiva para a privacidade dos usuários e se entende que essas são as duas únicas autoridades administrativas investidas de competência legal para requisitar dados cadastrais sem ordem judicial no âmbito de investigações destes crimes. Em outros casos, a ordem judicial ainda seria necessária para a entrega de dados cadastrais.

1.4 Entretanto, algumas autoridades policiais, em razão da Lei nº 12.830/2013, que dispõe sobre a investigação criminal conduzida pelo delegado de polícia, reivindicam autoridade de requisitar informações, independentemente do crime investigado (art. 2, §2º). Nesse aspecto específico, caso haja mudança da política nacional ou determinação do STF, essa política de privacidade poderá sofrer alterações. Por enquanto, fica estabelecido que:

a) A xx promete obedecer a legislação vigente ao fornecer dados de clientes a autoridades públicas.

b) A xx promete fornecer dados cadastrais por requisição (sem ordem judicial) apenas a autoridades administrativas competentes, identificando-as. Em outros casos, a xx exige ordem judicial.

c) A xx promete fornecer registros de conexão apenas mediante ordem judicial.

d) A xx faz uso de CG-NAT em sua rede.

e) A xx contesta todo e qualquer pedido abusivo de acesso a dados de usuários, ou seja, aqueles que extrapolavam as prerrogativas legais da autoridade autora do pedido e/ou eram desproporcionais, em razão de sua falta de clareza e precisão sobre dados requeridos e motivação, ou por qualquer outra razão que comprometa o direito à privacidade de usuários. O Decreto nº 8.771/2016 estabelece que as autoridades

administrativas devem indicar o fundamento legal de sua competência, a motivação do pedido de dados e que são vedados pedidos coletivos que sejam genéricos ou inespecíficos.

Dos Direitos dos Clientes:

1 - A xx disponibiliza o canal de atendimento xxxx a fim de que o cliente possa exercer seus direitos de acesso e cancelamento de recebimentos de mensagens de cunho publicitário.

2 - A manutenção das informações dos usuários observam os prazos legais previstos no Marco Civil da Internet e durante o tempo necessário para a prestação adequada do serviço contratado.

3 - As senhas fornecidas pela xx são de uso pessoal e intransferível: não devem ser compartilhadas com ninguém para segurança e proteção das suas informações.

3.1. Ao criar suas senhas, lembre-se de adotar um maior rigor, criando senhas com no mínimo oito caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais.

3.2. Mantenha sempre ativo e atualizado um antivírus de sua confiança, em todos os seus dispositivos que acessam a internet.

4 - A xxx recomenda que, caso o usuário do site seja menor de 18 anos, informe aos pais ou responsáveis sobre sua intenção de solicitar contato de nossa empresa ou assinar qualquer lista de email de nosso site. Recomendamos aos pais que se envolvam com a utilização da Internet por parte de seus filhos, certificando-se das atividades nas quais eles participam pela Rede.

5 - A xxx garante o direito de conhecimento e de opt-out das informações dos clientes e adotará os esforços razoáveis para atender à essa natureza de solicitação.

6 - Não há garantia de portabilidade de dados coletados pela xxx em função da coleta promovida e em razão do seu propósito específico para a prestação dos serviços.

7 - Os direitos do cliente não serão respeitados pela xxx caso haja qualquer inveracidade ou ilegitimidade através do uso indevido de informações de terceiros pelo cliente.

Do Encarregado:

1 – A xx informa que a encarregada pela proteção de dados na empresa é xxx, que poderá ser contatada pelo e-mail xxxx

2 – A xx se reserva o direito de alterar, a qualquer tempo, essa Política de Privacidade.

3 - Se você tiver qualquer dúvida sobre nossa política de privacidade, por favor, contate-nos pelo e-mail: xxxxx

Para Cookies:

Utilizamos cookies para melhorar a sua experiência de navegação. Se você estiver de acordo, basta que continue a navegar no site. Para mais informações, acesse nossa política de privacidade.

Para envio de Formulário:

Ao preencher o formulário com os dados cadastrais, o cliente está de acordo com o uso dos dados para o caso de contratação de plano ou envio de ofertas de serviço pelo XXX.

Anexo IV: Contrato de trabalho com colaborador

"O Empregado está de acordo com o coleta, uso, tratamento e armazenamento de seus dados pessoais e dados sensíveis pelo XXX, conforme exigido pelo eSocial, em função da execução do contrato de trabalho e cumprimento de obrigação legal. Entende-se como dados pessoais: Nome, endereço, RG, CPF, telefone, e-mail, data de nascimento e informações financeiras. Considera-se dados sensíveis: dados relacionados à saúde do titular e dependentes e etnia. A coleta e o tratamento de dados observam a obrigação de privacidade e seu uso submete-se a exigência legal. "

CONTATOS

ABRINT - Associação Brasileira de Provedores de Internet e Telecomunicações
CNPJ: 11.369.542/0001-52 - I.E – isento
Endereço: SCS quadra 01, Bloco G, Sala 1503, Ed. Baracat
Brasília - DF - CEP: 70.309-900 - Telefone: (61) 3039-1060

E-mails:
Administrativo e Financeiro: administrativo@abrint.com.br
Comunicação e Relacionamento
Institucional: gerente@abrint.com.br
Eventos: vivian@abrint.com.br
Jurídico: juridico@abrint.com.br

Listas:
abrint-associados@listas.abrint.com.br
abrint-juridico@listas.abrint.com.br
abrint-fornecedores@listas.abrint.com.br
abrint-tecnica@listas.abrint.com.br

abrint.com.br
Facebook: /abrintOficial
Instagram: /abrintoficial/
YouTube: /AbrintOficial
Linkedin: /company/abrintoficial

CLUBEDEMÍDIA

www.abrint.com.br