# Norma Técnica
# ABRADI/Bureau Veritas

# Proteção de Dados Pessoais

Novembro/2019

**ABRADI - Associação Brasileira dos Agentes Digitais**
R. Oscar Freire, 2379 - Pinheiros - São Paulo - SP - CEP 05409-012
Telefone: 0800 878 1212 - www.abradi.com.br

**Bureau Veritas Certification**
Av. Alfredo Egídio de Souza Aranha ,100 - Vila Cruzeiro - São Paulo - SP - CEP: 04726-170
Telefone: 11 2655-9000 - www.bureauveritascertification.com.br

# Sumário



 

# Prefácio

A Norma da Associação Brasileira dos Agentes Digitais e Bureau Veritas Certification (ABRADI/BUREAU VERITAS) de Proteção de Dados Pessoais constitui a autorregulamentação dos Agentes Digitais perante a Lei Geral de Proteção de Dados Pessoais (Lei n° 13.907/18) sancionada em 2018 e modificada pela Lei n° 13.853/19.

O propósito desta norma é apontar quais as obrigações e condutas os Agentes Digitais precisam cumprir e adotar para se adequarem e garantirem a efetiva proteção de dados pessoais aos seus titulares, bem como para que possam exercer com segurança jurídica suas atividades que envolvam a circulação de dados pessoais, de modo a estarem capacitados para serem submetidos à respectiva certificação.

A presente norma de autorregulamentação, considerando a finalidade da ABRADI de Zelar pelo cumprimento da legislação que rege a comunicação para o ambiente digital no Brasil, representa a preocupação do setor em se adequar e promover a valorização do mercado de comunicação digital por meio do equilíbrio entre a circulação de dados e a privacidade e proteção dos dados pessoais.

Esta Norma utiliza requisitos delineados pela Norma Técnica Bureau Veritas - Proteção de Dados Pessoais.

 

# 1 Definições

Nesta seção são apresentadas as definições de conceitos utilizados ao longo da norma, considerando os parâmetros legais, bem como os conceitos previstos na Norma Técnica Bureau Veritas de Proteção de Dados Pessoais (requisito 3).

## 1.1 Dado Pessoal

informação relacionada a pessoa natural identificada ou identificável (art.5º, I, Lei nº 13.709/18).

NOTA: São exemplos de dados pessoais CPF, RG, profissão, IP e COOKIE, entre outros dados que nos permitam identificar alguém;

## 1.2 Dado Pessoal Sensível

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art.5º, II, Lei nº 13.709/18).

NOTA: Muitas vezes, apesar de o dado pessoal demandar certa confidencialidade e dever de sigilo, como é o caso dos dados bancários e perfis de compras, nem sempre estes serão tratados como sensíveis pela LGPD;

## 1.3 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 (art.5º, III, Lei nº 13.709/18).

NOTA: Sendo assim, dados anonimizados não são considerados dados pessoais, não estando sujeitos às aplicações da lei;

## 1.4 Titular

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art.5º, IV, Lei nº 13.709/18);

## 1.5 Tratamento de dados pessoais

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 (art.5º, X, Lei nº 13.709/18).

NOTA: Assim, toda a operação que envolva informações capazes de identificar alguém direta ou indiretamente é considerada tratamento de dados pessoais, por exemplo: o serviço de tratamento e de duplicação de dados (*data quality*), a seleção de públicos para campanhas, o desenvolvimento de modelos e algoritmos com dados de clientes, o enriquecimento de bancos de dados com listas externas e os serviços de geolocalização;

### 1.6 Agentes de tratamento/Agente Digital

controlador e o operador (art.5º, IX, Lei nº 13.709/18);

### 1.7 Controlador

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art.5º, VI, Lei nº 13.709/18);

### 1.8 Operador

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art.5º, VII, Lei nº 13.709/18);

### 1.9 Encarregado de dados pessoais

pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (art.5º, VIII, Lei nº 13.709/18);

### 1.10 Consentimento

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art.5º, VIII, Lei nº 13.709/18);

### 1.11 Transferência Internacional de Dados

transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (art.5º, XV, Lei nº 13.709/18);

### 1.12 Relatório de Impacto à proteção de dados pessoais

documentação do controlador que identifica, descreve e classifica processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art.5º, XVII, Lei nº 13.709/18);

### 1.13 *Privacy by design* (privacidade desde a concepção)

utilização de mecanismos de privacidade em todo o ciclo do dado a ser tratado. A privacidade deve ser incorporada ao desenho do produto ou serviço, de modo a assegurar todo o fluxo do dado, desde a coleta até o término do tratamento (art.25, 1, GDPR).

### 1.14 *Privacy by default* (privacidade por padrão)

introduz a privacidade como modelo de conduta, de modo a minimizar processamento de dados pessoais, pela adoção de técnicas como a pseudoanonimização e criptografia.

 

## 2 Agentes de Tratamento

As disposições desta norma são dirigidas aos “agentes de tratamento” - controlador e operador. “Controlador de dados” é o responsável por tomar decisões acerca do tratamento de dados, já o “operador de dados” segue as instruções daquele, operacionalizando, tão somente, o tratamento dos dados pessoais, não devendo exceder ao que lhe foi determinado.

É importante se atentar à diferenciação dos papéis desempenhados no tratamento de dados pessoais, posto que o papel determinará quais requisitos se aplicarão à sua atuação e quais serão as possíveis responsabilizações pelo tratamento de dados. No caso do controlador, todos os requisitos apresentados nesta norma serão aplicáveis, enquanto para o operador podem variar, conforme tabela a seguir:

| Requisitos | Aplicabilidade para o operador |
|---|---|
| 3. Coleta de dados | Aplicável quanto às obrigações não pontuadas como exclusivas do controlador |
| 3.1. Consentimento | Aplicável |
| 3.2. Legítimo Interesse | Aplicável |
| 3.3. Organização dos dados | Aplicável |
| 4. Transparência no Uso dos Dados | Aplicável quanto às obrigações não pontuadas como exclusivas do controlador |
| 5. Compartilhamento de dados | Aplicável quanto às obrigações não pontuadas como exclusivas do controlador |
| 6. Transferência Internacional de Dados | Aplicável |
| 7. Incidente de Dados | Aplicável |
| 8. Anonimização & Exclusão dos Dados | Aplicável |
| 9. Boas práticas/Obrigações legais mitigadoras | Aplicável |

Quando o tratamento de dados envolver a subcontratação de um parceiro, como determina o art.28, do GDPR (*General Data Protection Regulation*) e art.39 da LGPD, a subcontratação deverá ser regida por instrumento contratual que vincule as partes, de modo que este indique o objeto, duração, natureza e finalidade do tratamento de dados pessoais, além das categorias dos titulares de dados pessoais, obrigações e direitos do controlador. Segundo este mesmo dispositivo da legislação europeia, o subcontratado deverá ainda cumprir com as devidas delimitações:

a) Não tratar dados pessoais de forma diversa das instruções documentadas pelo controlador e agir somente conforme o determinado por este;

b) Exigir e assegurar que os seus funcionários e demais pessoas que tratem dados pessoais tenham assumido compromisso de confidencialidade para fazê-lo;
c) Adotar medidas de segurança aptas e capazes de assegurar um nível de segurança adequado;
d) Em todo o tratamento considerar a sua natureza, prestando, sempre que possível, assistência técnica e organizativa adequada ao controlador (contratante);
e) Após a conclusão do contrato de subcontratação de prestação de serviços, proporcionar ao controlador (contratante) a escolha acerca da destinação dos dados pessoais com ele compartilhados: exclusão ou devolução dos dados pessoais. Eventuais cópias deverão ser apagadas, a menos que a conservação se dê por obrigação legal; e,
f) Cooperar com o controlador (contratante), disponibilizando as informações e os registros necessários a demonstrar o cumprimento das obrigações legais e contratuais assumidas, bem como contribuindo e colocando-se à disposição em caso de auditorias e inspeções, internas ou externas.

A Gestão de riscos de dados pessoais deve atender as cláusulas 5.1, 5.2 e 5.3 da Norma Técnica Bureau Veritas - Proteção de Dados Pessoais. Quando a subcontratação de serviços for aplicável, esta deve ser controlada conforme o requisito 8.2 da Norma Técnica Bureau Veritas – Proteção de Dados Pessoais.

 

## 3 Coleta de dados

Os agentes digitais devem adequar a coleta e o tratamento de dados pessoais ao disposto na Lei Geral de Proteção de Dados e demais legislações específicas relacionadas ao tema[1]. Como ponto de partida, é necessário entender que, segundo a LGPD, os dados coletados pertencem ao indivíduo ao qual dizem respeito.

Dessa forma, o tratamento de dados pessoais deve se restringir a propósitos legítimos e a finalidade específica informada ao titular de dados pessoais, no momento da coleta.

O Agente Digital, quando atuar como "controlador", deve se ater, também, no momento da coleta, ao **Princípio da Transparência**, que está intimamente ligado com a **visibilidade e acessibilidade** da informação. Assim, o titular de dados deve ficar ciente, neste momento, a respeito de quais dados serão coletados, com qual finalidade serão tratados, com quem serão compartilhados e quais são as hipóteses de exclusão.

Além disso, o tratamento de dados somente será lícito caso o Agente Digital o faça de acordo/fundado em uma das bases legais da LGPD, devendo este escolher a mais adequada entre as seguintes:

a) consentimento (escrito ou por meio que demonstre a vontade do titular);
b) cumprimento de obrigação legal;
c) necessidade para execução contratual;
d) exercício regular de direitos em processo judicial, administrativo ou arbitral;
e) proteção à vida ou incolumidade física do titular ou de terceiros;
f) para a tutela da saúde;
g) para atender a legítimo interesse do controlador (quem exerce poder de decisão sobre o tratamento dos dados) ou terceiro;
h) para a proteção de crédito; e,
i) em razão da publicidade dada aos dados por seu titular ou do acesso público irrestrito a este, desde que observados a finalidade com que o dado fora disponibilizado, a boa-fé e não fira direitos e garantias fundamentais.

Para que seja atendido o princípio da prestação de contas, o Agente Digital deve manter registros de suas operações referentes a dados pessoais. Em casos de coletas realizadas pelo legítimo interesse, se faz necessário elaborar um Relatório de Impacto de Proteção de Dados Pessoais sobre aquele determinado tipo de operação, de modo a arquivá-lo para fins de eventuais fiscalizações.

O Relatório de Impacto de Proteção de Dados Pessoais deverá conter: (i) a descrição dos processos de tratamento de dados pessoais e os tipos de dados coletados; (ii) a metodologia utilizada para a realização da coleta e para a garantia da segurança da informação; e (iii) a análise do controlador com relação às medidas de mitigação de risco (art.38, parágrafo único).

Falta: metodologia utilizada para classificar e pontuar os riscos e o risco residual remanescente após o tratamento mitigatório

[1] Constituição Federal, Código Penal, Código Civil, Marco Civil da Internet, Decreto do Marco Civil da Internet, Código de Defesa do Consumidor, Decreto E-commerce, Lei de Direitos Autorais, Lei de Cadastro Positivo, Decreto Cadastro Positivo, Lei de Acesso à Informação, Decreto Acesso à Informação, Lei do Sigilo Bancário, Lei Geral de Telecomunicações, Lei de Cadastros dos usuários de telefones pré-pagos, Regulamento do SCM/Anatel, Lei de Interceptação, Lei das Organizações Criminosas, Lei do Tráfico de Pessoas, Inserção de dados falsos na Administração Pública, Lei de Invasão de Dispositivo, Política de Segurança Cibernética – BACEN e Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais).

Além dos requisitos descritos acima, é obrigatório o atendimento dos requisitos descritos nas cláusulas 4.1, 4.2, 4.2.1 e 4.2.2 da Norma Técnica Bureau Veritas - Proteção de Dados Pessoais.

Independente da base legal utilizada pelo Agente Digital no tratamento de dados pessoais, este sempre deverá informar o titular de dados pessoais, de forma clara e transparente, como seus dados pessoais serão processados, além de outras informações, tais como:

a) Nome do Agente Digital
b) Contato do Encarregado de Dados Pessoais
c) Informação sobre a possibilidade de utilização dos dados para Marketing
d) Categorias de Dados Pessoais coletados
e) Propósito do tratamento dos dados coletados
f) Categorias de receptores de dados
g) Especificação e Identificação mínimas dos terceiros com quem os dados pessoais coletados eventualmente serão compartilhados
h) Locais de armazenamento e tratamento de dados hospedados em outros países
i) Período de armazenamento dos dados pessoais
j) Informação sobre os direitos do usuário e o canal para este exercê-los
k) Lembrete da possibilidade de revogação do consentimento a qualquer tempo

A transparência para com o titular de dados e sua compreensão em relação aos termos da Política de Privacidade são de suma importância, devendo ser esta redigida de forma clara e em linguagem acessível.

O tratamento de dados pessoais deve atender os requisitos 8.1 e 8.2 estabelecidos na Norma Técnica Bureau Veritas – Proteção de Dados Pessoais.

## 3.1 Consentimento

O consentimento, como visto anteriormente, é apenas uma das bases legais a fundamentar o tratamento de dados pessoais. Sendo assim, é necessário coletar e manter o registro do consentimento quando o tratamento não se encaixar em nenhuma das demais bases legais de tratamento. Por exemplo, uma empresa que capture dados para fins de prevenção às fraudes não necessitaria da coleta do consentimento, visto que "proteção ao crédito" é uma das bases legais.

Considerando o enfoque da Lei Geral de Proteção de Dados, o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art.5º, XII, da LGPD).

Estas expressões foram bem delimitadas pelo Parecer 15/2011 sobre a definição de consentimento do Grupo de Trabalho de Proteção de Dados do artigo 29º (referência à Diretiva Europeia revogada pelo GDPR), de modo que, segundo este parecer, adotado como parâmetro para o entendimento destes termos, consentimento livre, informado e inequívoco implica em:

> *""<<...**livre**...>>*
>
> ***O consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha** e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado. Se as consequências do*

 

> *consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre.*
>
> *(...)*
>
> *<<...**informada**...>>*
>
> ***A pessoa em causa deve receber, de forma clara e compreensível, informações exatas e completas sobre todas as questões pertinentes** (...), como a natureza dos dados tratados, as finalidades do tratamento, os destinatários das eventuais transferências e os seus direitos. Isto implica igualmente a consciência das consequências do não consentimento do tratamento em questão.*
>
> *(...)*
>
> *A exigência de um consentimento inequívoco não se coaduna com procedimentos para a obtenção de consentimento baseados numa omissão ou no silêncio das pessoas: ao silêncio ou omissão de uma pessoa está inerente uma ambiguidade (a pessoa em causa pode ter pretendido dar o seu assentimento ou pode simplesmente ter desejado não praticar o ato*
>
> *(...) **inequívoco**(...)*
>
> *a manifestação pela qual a pessoa aceita que os seus dados sejam objeto de tratamento deve ser inequívoca quanto à sua intenção. **Se existir uma dúvida razoável quanto à intenção da pessoa, existirá ambiguidade**.*
>
> *(...) este requisito obriga os responsáveis pelo tratamento a criar procedimentos rigorosos para as pessoas em causa prestarem o seu consentimento, nomeadamente procurando obter o consentimento expresso ou baseando-se em tipos de procedimentos a partir dos quais o consentimento possa claramente ser inferido. O responsável pelo tratamento deve também assegurar-se de que a pessoa que presta o consentimento é, efetivamente, a pessoa em causa, o que assume particular relevância quando o consentimento é prestado por telefone pela internet."[2].*

Assim, no momento da coleta do consentimento deverá ser informado e registrado:

a) a finalidade específica do tratamento;
b) com quem, eventualmente, aquele dado pessoal será compartilhado;
c) qual será o período de duração do tratamento;
d) a informação da possibilidade de não fornecer o consentimento; e,
e) quais seriam as consequências da negativa.

Não são permitidos, como manifestação de consentimento válido, comportamentos de omissão (*opt-out*), como caixas previamente assinaladas, ou que apresentem finalidades genéricas para o tratamento de dados pessoais, dentre outras práticas que não coadunam com uma manifestação livre, informada e inequívoca.

O Agente Digital, quando for responsável pela coleta, deve, ainda, manter os registros que comprovem a concessão do consentimento bem como que este se deu de forma livre, informada e inequívoca. Esta guarda de registros é necessária para atendimento do Princípio da Responsabilização e Prestação de Contas, segundo o qual é necessária a demonstração,

[2] http://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf, acessado em 29 de novembro de 2015.

pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art.6º, X, da LGPD).

Os registros devem ser capazes de comprovar:

a) O consentimento;
b) As informações concedidas e a finalidade divulgada ao titular de dados, quando do momento da coleta do consentimento;
c) Por qual mecanismo e forma o consentimento se deu e, quando possível, apresentar registro com horário e data do consentimento;
d) Apresentar cópias dos registros de coleta de dados feitos on-line e off-line por período razoável;
e) Produzir registro de auditoria de como e quando o consentimento foi dado como forma de evidência, caso solicitado; e
f) Apresentar registros de revogação do consentimento, ou de invalidação por alteração das circunstâncias.

### 3.2 Legítimo interesse

Se a base legal para fundamentar o tratamento de dados pessoais a ser realizado pelo Agente Digital for o legítimo interesse, este deve se adequar às hipóteses previstas na LGPD: (i) para apoiar e promover atividades do controlador; e (ii) para proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem o usuário (art.10º, I e II, LGPD).

O GDPR, em seu artigo 47, igualmente eleva a legítimo interesse o tratamento de dados realizado com fins de prevenção à fraude ou para efeitos de comercialização direta, desde consideradas as seguintes condições:

a) existência de relacionamento pré-existente com o titular de dados pessoais;
b) expectativa razoável do titular de dados (previsibilidade);
c) garantia da oportunidade de cancelamento ou recusa do tratamento.

Além disso, o Agente Digital deve observar e respeitar os seguintes parâmetros legais:

a) somente utilizar os dados estritamente necessários para a finalidade pretendida;
b) quando atuar como controlador, adotar todas as medidas para garantir a transparência no tratamento em relação ao titular de dados;
c) elaborar e arquivar Relatório de Impacto à Proteção de Dados Pessoais;
d) garantir que o legítimo interesse não se sobrepõe aos direitos individuais do titular dos dados.

### 3.3 Organização dos dados

A fim de atender eventual fiscalização da Autoridade de Proteção de Dados Pessoais ou solicitação de acesso por parte dos titulares de dados pessoais, os Agentes Digitais deverão organizar os bancos de dados pessoais.

a) Os Agentes digitais deverão, nesse sentido, gerir os bancos de dados pessoais, de modo que seja possível rastrear as informações com o intuito principal de garantir

 

direitos, sendo certo que para tanto deverão: Classificar os dados de acordo com a origem, finalidade e base legal para o tratamento de dados pessoais;

b) Registrar os critérios utilizados no tratamento dos dados;
c) Guardar registros do consentimento, quando aplicável;
d) Arquivar Relatório de Impacto de Proteção de Dados Pessoais, que demonstre o raciocínio jurídico para a utilização do legítimo interesse, quando aplicável;
e) Além de outros critérios utilizados pela organização e delimitados em Política Corporativa de Privacidade e Proteção de Dados Pessoais.

## 4 Transparência no Uso dos dados

O uso dos dados, independente da base legal que o embase, deve ser realizado em conformidade com a finalidade previamente informada ao titular, com a garantia de que seus dados serão utilizados somente para propósitos legítimos, específicos, explícitos e informados, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Quando a finalidade atribuída para tratamento dos dados for alterada, deverá o agente digital, caso atue como "controlador", informar ao titular sobre as alterações, podendo o titular, caso discordar com a nova finalidade, requerer a revogação de seu consentimento. Caso a base legal para a coleta tenha sido o consentimento, será necessário solicitar novo consentimento diante da alteração da finalidade.

A necessidade de transparência do controlador perante o uso dos dados coletados é imprescindível. As informações sobre o tratamento de dados devem ser claras, adequadas e ostensivas, de forma que o titular dos dados tenha a plena capacidade de compreender tudo.

Seguindo tal princípio, o agente digital, no papel de "controlador", que realiza o tratamento de dados tem o dever de garantir os direitos dos titulares dos dados de:

a) Confirmação de existência de tratamento dos dados;
b) Acesso aos dados;
c) Correção de dados;
d) Anonimização e eliminação dos dados;
e) Portabilidade dos dados, resguardados os segredos comerciais;
f) Informação sobre a possibilidade de revogação/retirada do consentimento;
g) Possibilidade de revogação do consentimento, a qualquer tempo mediante solicitação.

Quando o titular dos dados solicitas o acesso aos seus dados, o agente digital deve providenciar, dentro do prazo legal, o acesso facilitado das informações, que deverão necessariamente apresentar: (i) finalidade específica do tratamento; (ii) forma e duração do tratamento; (iii) identificação do controlador;(iv) informações de contato do controlador; (v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (vi) responsabilidades dos agentes que realizarão o tratamento; e (vii) direitos do titular, citados acima.

A transparência se mostra igualmente imprescindível na prática do tratamento denominado *Profiling*, o qual envolve processamento automatizado, dados pessoais e avaliação de aspectos pessoais. Além de estar fundado em uma base legal, esta prática deve estar sempre atrelada a (i) medidas para identificar e solucionar imprecisões; (ii) segurança apropriada; (iii) prevenção de efeitos discriminatórios; (iv) minimização dos dados; (v) pseudoanonimização; (vi) processos de intervenção humana.

As funções, responsabilidades e autoridades na organização devem ser definidas conforme estabelecido nos requisitos 4.3, 4.3.1 e 4.3.2 da Norma Bureau Veritas – Proteção de Dados Pessoais.

 

# 5 Compartilhamento de dados

O Agente Digital deve garantir, ao compartilhar dados com terceiros ou outras empresas de seu grupo econômico, que todos estes estejam de acordo com a sua política de privacidade e práticas de segurança, garantindo o mesmo nível de adequação à proteção de dados pessoais.

As partes envolvidas no compartilhamento devem ser capazes de garantir a segurança dos dados desde sua coleta até sua exclusão de toda a cadeia. Sendo assim, todos os envolvidos no compartilhamento deverão garantir a segurança dos dados pessoais em nível adequado.

O agente de tratamento de dados pessoais, classificado como “controlador”, que os compartilhar será responsável por garantir que: (i) os dados compartilhados foram coletados de maneira lícita e regular; (ii) que os titulares dos dados foram informados e têm ciência acerca do compartilhamento e suas condições; (iii) há registros válidos do consentimento destes titulares de dados, quando aplicável.

O compartilhamento de dados pessoais entre parceiros, as suas condições e nível de adequação exigidos devem ser objeto do instrumento contratual que regerá a relação entre os dois agentes de tratamento de dados pessoais. O Agente Digital deve sempre se certificar do nível de adequação à proteção de dados e segurança de seus parceiros, sendo recomendável que exerça fiscalizações e controles periódicos a respeito.

O tratamento de dados não fundado em base legal é irregular, assim, se um agente de tratamento mantiver ou obtiver dados pessoais dessa forma, esta coleta deverá ser interrompida, obstando-se, assim, a transmissão destes dados pessoais.

Quando o Agente Digital receber dados pessoais de outrem deverá exigir a declaração de regularidade do registro da origem e da finalidade divulgada relacionada aos dados fornecidos.

## 6 Transferência Internacional de Dados

Os Agentes Digitais que realizam transferência de dados pessoais para outros países devem se ater às regras da transferência internacional de dados, vez que esta prática é limitada pela legislação nacional.

Para que a transferência internacional de dados pessoais se dê em conformidade com a LGPD, esta precisará se enquadrar em uma das hipóteses abaixo (art.33, LGPD):

a) Transferência para países ou organismos internacionais que proporcionem nível adequado de proteção de dados pessoais;
b) Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei de Proteção de Dados, na forma de:
    1. cláusulas contratuais específicas para determinada transferência;
    2. cláusulas-padrão contratuais;
    3. normas corporativas globais;
    4. selos, certificados e códigos de conduta regularmente emitidos;
c) Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, tudo nos conformes com os instrumentos de direito internacional;
d) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
e) quando a autoridade nacional autorizar a transferência;
f) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
g) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público
h) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo-a claramente de outras finalidades
i) quando necessário para cumprimento de obrigação legal; para execução de contrato; e exercício de direitos.

Além de ser necessário o enquadramento em uma das hipóteses acima, será preciso verificar as demais legislações incidentes no tratamento de dados pessoais, considerando as normas dos demais países/regiões envolvidos no respectivo tratamento.

 

# 7 Incidente de dados

Ao detectar qualquer violação de dados pessoais em suas áreas ou parceiros, o Agente Digital deverá informar o Encarregado de Dados ou responsável pelo tratamento na empresa, bem como o Encarregado de Dados do Controlador do tratamento, tão logo identifique a violação. Caso o Agente Digital possa ser classificado como controlador e a violação tiver potencialidade de danos aos titulares, deverá ainda notificar a Autoridade Nacional de Proteção de Dados Pessoais – ANPD dentro do prazo legal.

A notificação destinada à ANPD deverá conter (art.48, LGPD):

a) a descrição da natureza dos dados pessoais afetados;
b) as informações sobre os titulares envolvidos;
c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
d) os riscos relacionados ao incidente;
e) os motivos da demora, no caso de a comunicação não ter sido imediata; e
f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

O gerenciamento de violação de dados deve atender ao requisito 5.4 da Norma Técnica Bureau Veritas – Proteção de Dados Pessoais.

## 8 Anonimização & Exclusão dos Dados

Esta norma, assim como a LGPD, não é aplicável aos dados anonimizados, salvo quando o processo de anonimização puder ser revertido por meio de esforços razoáveis. Desta forma, a anonimização dos dados pessoais se torna uma opção aos agentes de tratamento que queiram, por exemplo, para fins estatísticos e de direcionamento de campanhas, manter o tratamento de dados.

Da mesma forma, como as demais práticas, a realização de campanhas por dados de geolocalização não foi inviabilizada pela LGPD. Se estes dados estiverem anonimizados, ou seja, o seu titular não puder ser identificado por esforços técnicos razoáveis, não há impedimento, visto que dados anonimizados não são considerados como dados pessoais, de forma que a LGPD não se aplica a estes.

No entanto, como já sinalizado, caso seja possível a identificação do indivíduo, os dados de geolocalização estarão sob o manto da LGPD e a estes deverão ser destinados os mesmos cuidados do que os demais dados pessoais.

O tratamento de dados pessoais deverá sempre ser restrito ao necessário para a consecução da finalidade divulgada no momento da coleta sendo que, uma vez atingida a finalidade, deverão ser excluídos ou anonimizados. Caso a coleta tenha se dado por meio da base legal do consentimento, recomenda-se a renovação deste após atingimento da finalidade, a fim de evitar a fragilização desta base legal, fundamento do tratamento.

 

## 9 Boas práticas/Obrigações legais mitigadoras

Os Agentes Digitais precisarão adequar-se à LGPD. Assim, faz-se imprescindível estabelecer um cronograma de adequação para que seja possível cumprir a legislação, sendo certo que, os pontos abaixo, elencados no artigo 50 da LGPD, deverão fazer parte do *Programa Compliance* de qualquer Agente Digital e da implementação de programa de governança em privacidade que, no mínimo:

a) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) Conte com planos de resposta a incidentes e remediação;
h) Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; e
i) Inclua regras de boas práticas e de governança publicadas e atualizadas periodicamente, sendo possível demonstrar a efetividade do programa quando apropriado.

O Agente Digital deve, ainda, estabelecer práticas de governança que atendam aos requisitos abaixo que estão estabelecidos na Norma Técnica Bureau Veritas – Proteção de Dados Pessoais:

- 6.1- Manual e procedimentos
- 6.2 – Informação documentada
- 6.3 – Avaliação de desempenho
- 6.5 – Não conformidade e ação corretiva
- 6.6 – Reclamações (controlador e operador)
- 6.7 – Análise crítica pela direção
- 6.8 – Comunicação
- 6.8.1 - Geral
- 6.8.2 – Comunicação Interna
- 9 - Recursos
- 9.1 – Infraestrutura
- 9.2 - Pessoal
- 9.2.1- Competência
- 9.2.2 - Conscientização