

MANUAL DE COMPLIANCE EM PROTEÇÃO DE DADOS

BTS – BUSINESS TRANSLATION SERVICES

FEVEREIRO - 2022

Sumário

PARTE 1 – ENTENDENDO A LGPD

1. Definições.....	3
2. Introdução	4
3. O que são Dados Pessoais?.....	4
4. O que é Tratamento de Dados Pessoais?	6
5. Quais são os princípios da LGPD?	6
6. Quem são os agentes de Tratamento?	7
7. O que é uma transferência internacional?	7
8. O que são bases legais?.....	7
9. O que é e o que faz o Encarregado ou DPO?	8
10. O que são direito dos titulares?	9

PARTE 2 – INSTRUÇÕES GERAIS SOBRE O CUMPRIMENTO DA LGPD

1. Mapeamento de dados (ref. Imagem número 1):	11
2. Aplicação dos Princípios (ref. Imagem número 2).....	11
3. Verificação/ aplicação da base legal (ref. Imagem número 3).	14
4. Atividades que acarretem risco (ref. Imagem número 4)	14
5. Privacy by Design e by Default	14
6. Aviso de transparência (ref. Imagem número 6).....	14
7. Transferências Internacionais (ref. Imagem número 7).....	14
8. Ciclo do Dado Pessoal (ref. Imagem número 8)	15
8.1.Diretrizes sobre a coleta e o processamento do dado pessoal:	15
8.2.Descarte e expurgo Dados Pessoais	15
9. Atendimento aos Direitos dos Titulares. (ref. Imagem número 9).....	16
10. Boas Práticas em geral (ref. Imagem número 11).....	16
11. Diretrizes sobre gestão de Terceiros (ref. Imagem número 12)	16
12. Segurança da Informação (Ref imagem 11 e 14)	16
13. Plano de Resposta a Incidentes de Segurança (Ref imagem 13 e 14)	17
14. Treinamentos (ref imagem: 11 e 14).....	17

Anexos

- 1.Anexo I- Modelo simples de Inventário de Dados
- 2.Anexo II -Modelo de Cláusula Contratual para Clientes.

PARTE 1

ENTENDENDO A LGPD

1. Definições

- **“Titular”** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **“Controlador”** significa qualquer pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais;
- **“Dados Pessoais”** significa qualquer informação relacionada a pessoa identificada ou identificável;
- **“Dados Pessoais Sensíveis”** significa qualquer 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;
- **“Encarregado”** significa a pessoa indicada pelo agente de Tratamento para atuar como canal de comunicação entre o agente de Tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **“Incidente”** significa qualquer ocorrência que, potencialmente ou efetivamente, ameace a confidencialidade, integridade ou disponibilidade dos dados tratados pela BTS e do sistema de informação da BTS. A ocorrência pode gerar uma violação ou ameaça as políticas de segurança, os procedimentos de segurança ou quaisquer outras políticas ou regras aplicáveis. Incidentes incluem, mas não se limitam à: (i) acesso indevido aos sistemas da BTS; (ii) acesso não autorizado aos Dados Pessoais tratados pela BTS; (iii) alteração ou perda de Dados Pessoais ou informações tratadas pela BTS; (iv) quaisquer outras falhas de segurança que possam resultar em acesso não autorizado aos sistemas da BTS, por meio de técnicas, conhecimento e ferramentas que explorem brechas específicas nos sistemas de informação;
- **“Novo Processo”** significa todo e qualquer Novo Processo, produto, serviço, projeto, atividade ou fluxo de trabalho que envolva o Tratamento de Dados Pessoais que não tenha sido previamente mapeado e informado aos Titulares de Dados Pessoais;
- **•“Controlador”** significa pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **“Operador”** significa qualquer pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador;
- **“Terceiro”** significa qualquer prestador de serviço, fornecedor, parceiro ou outro Terceiro que mantenha relação com a BTS;
- **“Tratamento”** significa 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.

2. Introdução

O objetivo desse manual (“**Manual**”) é indicar aos colaboradores da BTS conceitos sobre a Lei Geral de Proteção de Dados (“**LGPD**”) e como aplicá-los em seu dia a dia para, após, definir regras internas na BTS para garantir o cumprimento da Legislação Aplicável, em conformidade com seu Programa de Governança em Privacidade (“**Programa**”).

A LGPD entrou em vigor em setembro de 2020 para regular o uso de dados pessoais.

Apesar da lei trazer obrigações concretas em relação a controles e documentos que devem ser apresentados pelas Controladores e Operadores, é uma lei principiológica, ou seja, devem-se aplicar mecanismos para que os princípios sejam atingidos.

Um dos fundamentos mais importantes **da lei é a busca pela autodeterminação informativa do titular dos Dados Pessoais**, ou seja, a pessoa sobre quem os dados se referem. **Em outras palavras, os princípios, direitos e obrigações dessa lei buscam garantir que o titular do Dado Pessoal tenha conhecimento do uso que está sendo feito dos seus dados**, evitando violações à privacidade em razão de uso indevido de informações pessoais.

3. O que são Dados Pessoais?

Dado pessoal é toda e qualquer informação relacionada a uma pessoa natural identificada ou identificável, a qual chamamos de titular.

Quando falamos de dados referentes a uma pessoa natural **identificada**, nos referimos a uma informação que **permita identificar quem é aquela pessoa de maneira direta**. Nome, RG, CPF, endereço, telefone, login, carteira de trabalho, são alguns exemplos.

Agora, quando falamos de dados referentes a uma pessoa natural **identificável**, nos referimos a **informações** que, quando **associadas a outras**, podem identificar uma pessoa. Preferências pessoais, controle de ponto, cargo na empresa, geolocalização são alguns exemplos de dados que, de forma indireta, permitem identificar uma pessoa.

Também existem os Dados Pessoais Sensíveis, que são aqueles cujo uso indevido tem o potencial de ocasionar maiores danos aos titulares e gerar formas graves de discriminação. O Tratamento desses dados demanda

cuidados adicionais. Dados Pessoais Sensíveis são os dados de saúde, relativo as crianças, etnia, religião, orientação política, entre outros.

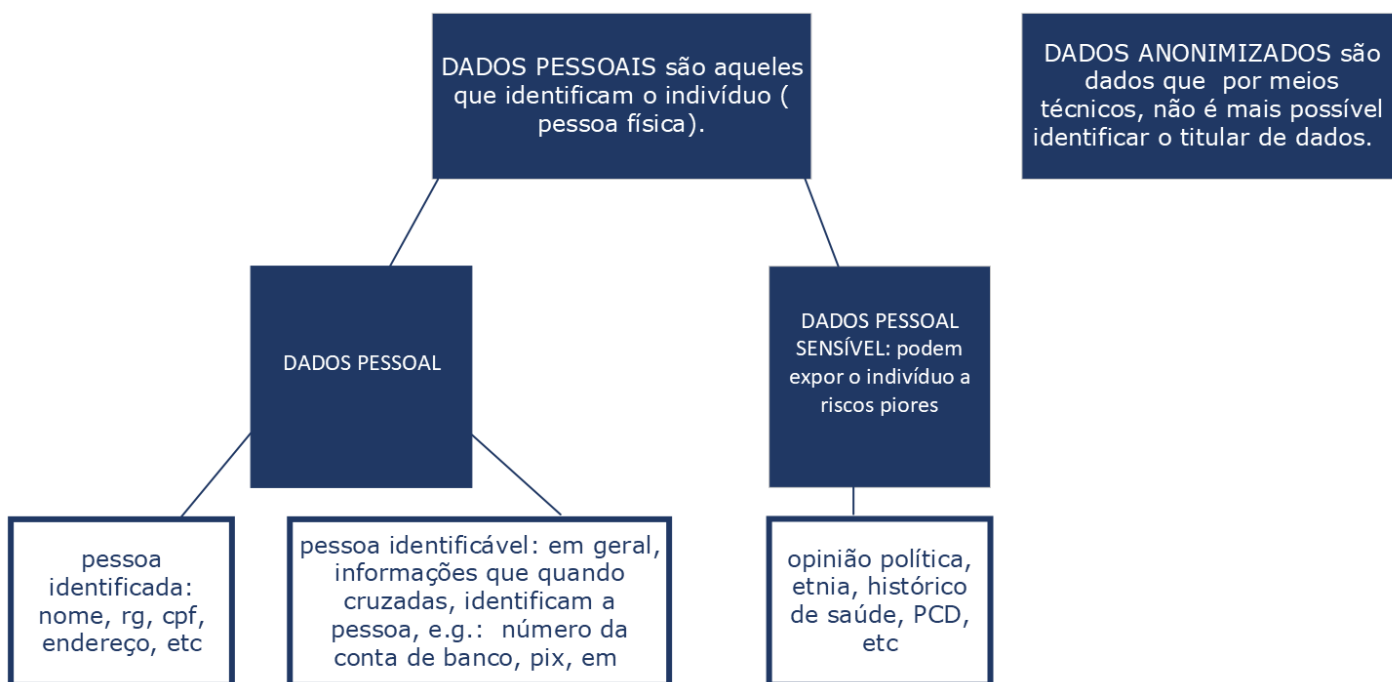


Atenção! Dados financeiros e bancários, apesar de potencialmente representarem um grande risco ao titular (ex.: dados de cartão de crédito vazados que são utilizados para fraude), na definição legal não são Dados Pessoais Sensíveis, apenas Dados Pessoais. É comum encontrar notícias sobre vazamentos de dados que confundem esses conceitos. Apenas aqueles listados acima são considerados, pela LGPD, como Dados Pessoais Sensíveis.

Os **Dados Pessoais pseudonimizados** são aqueles que passaram por um processo pelo qual o titular deixa de ser identificado diretamente. No entanto, o dado pode voltar a ser identificado por meio de um processo reversível ou dedução utilizando outros dados. Em resumo, o **dado parece anônimo, mas não é. Os dados pseudonimizados ainda estão sujeitos à LGPD.**

Já os **Dados Pessoais anonimizados** são aqueles que passaram por um processo a partir do qual a informação não permitirá mais que um indivíduo seja identificado. Ou seja, o processo para desassociar a informação da pessoa a que ela diz respeito não é reversível. Como **os dados anônimos não estão sujeitos à LGPD**, é importante ressaltar que para considerar um dado como anônimo, a empresa deve analisar diversos fatores e conduzir um estudo interno sobre tal fato.

Desta forma, temos:



4. O que é Tratamento de Dados Pessoais?

O Tratamento de Dados Pessoais **é qualquer operação com Dados Pessoais**. A LGPD menciona coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento, entre outros. Esse Tratamento pode ser conduzido por uma pessoa física ou por uma pessoa jurídica, como uma empresa ou associação, seja ela pública ou privada. O conceito engloba tanto os Dados Pessoais em suporte físico (como uma pasta de arquivo) quanto em suporte eletrônico (coleta de dados para informações, orçamentos através de um site ou serviço online e/ou processamento destas informações por meio de um software).

5. Quais são os princípios da LGPD?

Toda operação de dados deve obedecer aos princípios para o tratamento:

O **princípio da finalidade** estabelece que todo Tratamento deverá ser realizado com uma finalidade específica. Por exemplo, se o departamento de operações quiser coletar dados de clientes ou Terceiros específicos, deve haver um objetivo no uso desses dados, como o desenvolvimento de estatísticas e relatórios específicos ou o contato com determinados titulares para realizar uma pesquisa de satisfação.

Já o **princípio da necessidade** afirma que o Tratamento deve ser limitado ao mínimo necessário para sua execução. Em outras palavras, se o departamento de RH precisa documentar o afastamento de um empregado que teve uma virose, basta um atestado médico, não sendo necessário a entrega do prontuário médico completo do empregado.

O **princípio da transparência** é a garantia de que o titular saiba o que será feito com seus Dados Pessoais. Como exemplo podemos citar todas os Termos de Uso e Políticas/Avisos de Privacidade de aplicativos e serviços que explicam ao usuário como a empresa usa seus Dados Pessoais.

O **princípio da adequação** afirma que o Tratamento deve estar adequado às finalidades informadas ao titular. Ou seja, não se pode realizar um Tratamento que o titular não tenha tido a oportunidade de tomar conhecimento.

Já o **princípio da segurança** afirma que os responsáveis por Tratamentos devem utilizar medidas aptas a protegerem os Dados Pessoais de incidentes. Muito similar é o **princípio da prevenção**, o qual afirma que medidas capazes de prevenir danos causados em decorrência do tratamento de dados também devem ser adotadas.

Por fim, há o **princípio da responsabilização e prestação de contas**. A ideia é que quem trata dados seja capaz de adotar medidas para comprovar

que está cumprindo com a LGPD. Assim, é importante que os documentos relacionados à Dados Pessoais estejam organizados e atualizados, caso haja algum questionamento por titulares e/ou autoridades.

6. Quem são os agentes de Tratamento?

As pessoas, físicas ou jurídicas, que de qualquer forma interagem com o Tratamento de Dados Pessoais são chamadas *agentes de Tratamento*. A LGPD divide os agentes de Tratamento de Dados Pessoais, em 2 categorias:

Controlador: é o agente que toma as decisões sobre o Tratamento de Dados Pessoais. Portanto, o Controlador tem maiores responsabilidades quanto ao Tratamento, inclusive de zelar pela sua legalidade.

Operador: é o agente que realiza o Tratamento de Dados Pessoais em nome do Controlador.

Essa classificação é muito importante para compreender o papel de cada parte em um projeto que envolva Tratamento de Dados Pessoais, inclusive quando a BTS realiza contratos com Terceiros que realizem o Tratamento de Dados Pessoais, por exemplo: empresas de serviços em nuvem ou bancos de talentos.

7. O que é uma transferência internacional?

A transferência internacional de dados ocorre quando os dados são transferidos para outro País. A LGPD prevê alguns mecanismos de transferência que devem ser obedecidos quando houver transferência internacional. Muitos deles ainda precisam ser dirimidos pela Autoridade Nacional de Proteção de Dados.

As transferências de Dados Pessoais pela BTS a Terceiros fora do país só podem ser realizadas se cumpridos certos requisitos da LGPD, que buscam dar a tais Dados Pessoais e seus titulares uma proteção mínima.

Geralmente contratos de serviços em nuvem, *software as a service*, entre outros, incluem transferências Internacionais.

8. O que são bases legais?

Além de ter uma finalidade específica para o tratamento, os Dados Pessoais devem ter uma base legal para serem tratados licitamente. As bases legais estão estabelecidas em lei. Abaixo, incluímos as bases legais que entendemos estar mais próximas das atividades desenvolvidas pela BTS. Seguem as bases legais para dados pessoais:

- **Consentimento:** o consentimento deve ser específico para aquela atividade. Ainda, o titular deverá ser avisado que pode recolher seu consentimento a qualquer momento e a BTS deverá disponibilizar meios para a retirada do consentimento.
- **Execução do Contrato:** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato, do qual o Titular de dados seja parte.
- **Cumprimento de obrigação legal pelo Controlador:** quando aquele que realizar o Tratamento de dados é obrigado por lei a tratar estes dados, como por exemplo, quando é obrigado a guardar os dados ou compartilhá-los com as autoridades competentes (ex.: obrigações tributárias e trabalhistas).
- **Exercício regular de direito:** quando os dados são necessários para uma ação judicial ou administrativa ou para exercer um direito, de forma geral.
- **Interesses legítimos:** quando o responsável pelo Tratamento dos dados tem interesse legítimo no Tratamento sem violar os direitos fundamentais dos titulares.
- **Proteção do crédito:** quando necessário para evitar fraudes, golpes, etc.
- **Proteção da vida:** quando necessário para proteger a vida do titular ou de Terceiro
- **Estudos por órgãos de pesquisa:** quando necessários para realização de uma pesquisa por uma organização legítima.
- **Tutela da saúde:** quando necessário para a execução de serviços de saúde por prestadores de tais serviços.

9. O que é e o que faz o Encarregado ou DPO?

O Encarregado de Proteção de Dados ou *data protection officer* (“**Encarregado**” ou “**DPO**”) é a pessoa indicada pelo agente de Tratamento para ajudá-lo a cumprir a LGPD. Suas principais responsabilidades são:

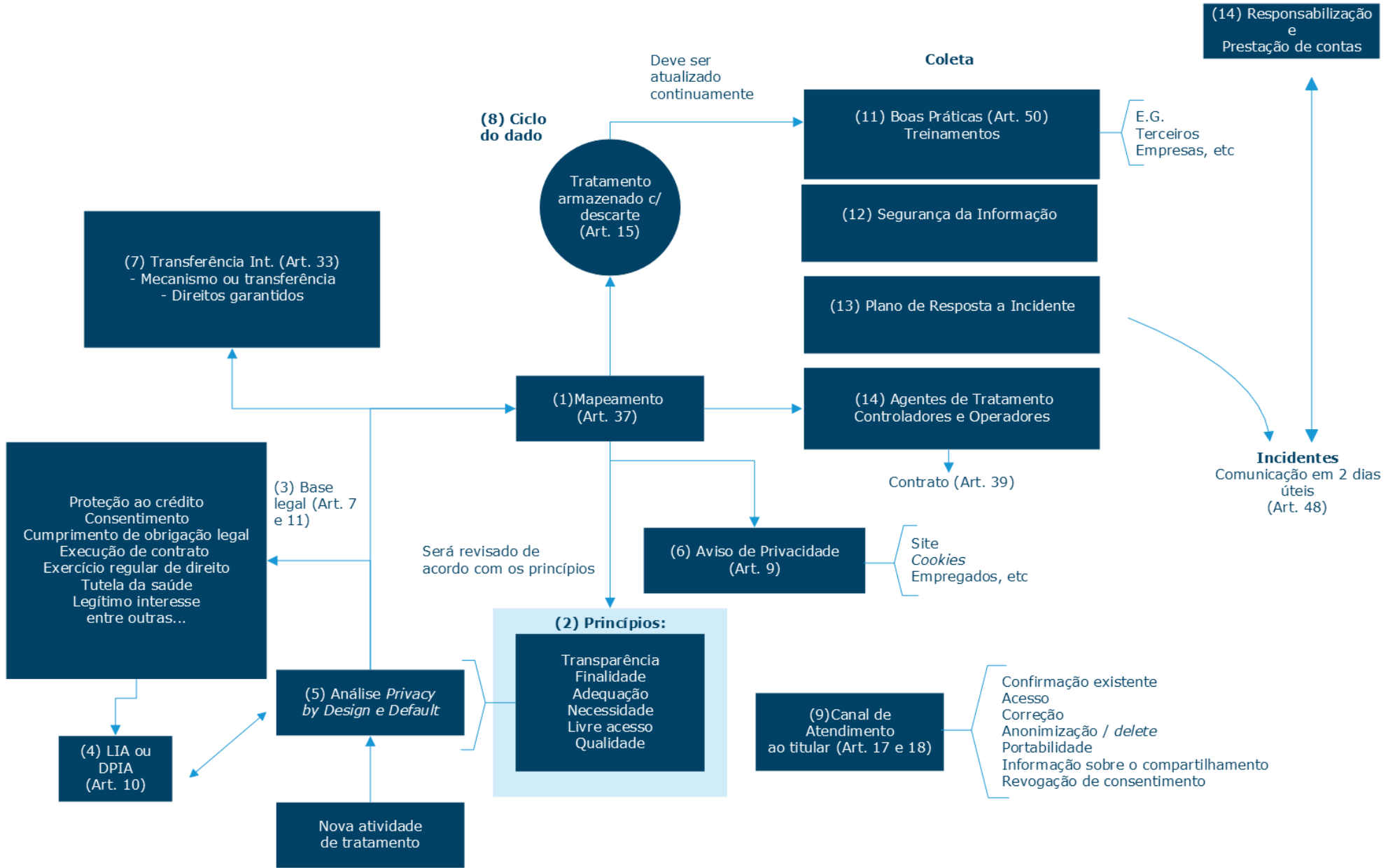
- Atuar como canal de comunicação com Titulares e com a ANPD
- Realizar análises de risco dos processos da BTS que envolvem Dados Pessoais
- Orientar os colaboradores sobre proteção de dados
- Aconselhar a empresa sobre o cumprimento da LGPD

10. O que são direito dos titulares?

Os titulares possuem direitos sobre os Dados Pessoais tratados. Dessa forma, o Controlador do Tratamento deve cumprir com esses direitos quando o titular faz uma solicitação. Por isso, se faz importante ao pensar em um tratamento de dados pessoais, em como será possível atender os direitos abaixo.

- **Confirmação da existência do Tratamento:** quando o titular deseja confirmar se o suposto responsável pelo Tratamento está de fato tratando seus dados.
- **Direito de acesso:** quando o titular pede para acessar quais os Dados Pessoais estão sendo tratados pelo responsável.
- **Correção de dados incompletos, inexatos ou desatualizados:** quando o titular identifica que há algum problema com seus dados e solicita a devida correção.
- **Portabilidade:** quando o titular solicita que seus dados sejam transferidos a um outro prestador de serviços.
- **Informação sobre compartilhamento de dados:** quando o titular solicitar informações sobre com quem o responsável compartilha seus Dados Pessoais e com quais finalidades.
- **Oposição, à exceção do consentimento:** quando o titular solicitar eliminação, anonimização ou bloqueio de dados desnecessários, excessivos ou Tratamentos em desconformidade com a LGPD.
- **Eliminação de dados tratados com base em consentimento:** quando o titular solicitar eliminação dos Dados Pessoais tratados com base em seu consentimento.
- **Informação sobre a possibilidade de não fornecer consentimento:** quando o titular questiona quais as consequências do não fornecimento de seu consentimento para o Tratamento de Dados Pessoais.

Fluxograma para entendimento de itens de adequação à LGPD



PARTE 2

INSTRUÇÕES GERAIS SOBRE O CUMPRIMENTO DA LGPD

1. Mapeamento de dados (ref. Imagem número 1):

A LGPD prevê que tanto o Operador como o Controlador devem manter registro das operações de tratamento de Dados Pessoais. Esse registro é o chamado mapeamento de dados, que é um processo vivo, ou seja, deve ser atualizado conforme novos processamentos sejam implementados ou excluídos.

O mapeamento é um instrumento que é utilizado para identificar fluxos de dados e determinar se os Tratamentos de dados estão ou não adequados. Ao mapear Dados Pessoais e armazenar esse registro, você cumpre com o primeiro quesito do diagrama acima e com o art. 37 da LGPD.

Para tanto, indicamos o preenchimento do arquivo de mapeamento de dados incluído a este documento como Anexo 1. Este mapeamento inclui informações gerais sobre o Tratamento de Dados Pessoais, como, por exemplo: Dados Pessoais coletados, meio de coleta, base legal, tempo de retenção destes dados, informações se estes são compartilhados com Terceiros (e quais são esses Terceiros), informações se existem transferência internacional, entre outros.

Após ao mapeamento dos processos, deverão ser realizadas as análises descritas a seguir. Estas mesmas análises deverão ser realizadas para Novos Processos, ou seja, toda vez que a BTS pensar em um novo processo de uso ou coleta de Dados Pessoais, deve antes analisar se os princípios abaixo elencados estão sendo respeitados e se existe uma base legal para o Tratamento.

2. Aplicação dos Princípios (ref. Imagem número 2)

Descrevemos cada Princípio na Parte 1, item 5 deste Manual. Qualquer atividade de Tratamento de Dados Pessoais que a BTS for realizar, deve respeitar os princípios da LGPD. Desta forma, para cada atividade mapeada, a BTS deverá avaliar conforme abaixo:

a) **Os Dados Pessoais somente são tratados se houver uma NECESSIDADE e uma FINALIDADE.** O Tratamento de Dados Pessoais deve ser condicionado à identificação de uma finalidade **legítima** e explícita que justifique o uso desses dados pela BTS.

b) **Os Dados Pessoais somente podem ser usados para atender uma finalidade identificada.** Os Dados Pessoais somente poderão ser usados

para a finalidade que justificou o seu Tratamento ou para uma finalidade adicional que seja compatível com a original.

c) **Deve ser usado o mínimo de Dados Pessoais necessário para atingir uma finalidade identificada.** No Tratamento de dados, somente se usará o mínimo de Dados Pessoais necessários para atingir a finalidade que justificou o Tratamento desses.

d) **Os Dados Pessoais devem ser usados de forma proporcional à finalidade identificada.** O Tratamento de Dados Pessoais deve ser realizado de modo proporcional à finalidade designada.

e) **Os Dados Pessoais não podem ser tratados de forma abusiva.** O Tratamento de Dados Pessoais não poderá ser realizado para fins discriminatórios ou abusivos.

f) Os Titulares devem ter **LIVRE ACESSO** aos seus dados.

g) **Os Dados Pessoais devem ser mantidos atualizados, sempre que possível.** Os Dados Pessoais tratados pela BTS devem estar sempre atualizados, exatos e claros.

COLOCANDO OS PRINCÍPIOS EM PRÁTICA

OPERAÇÃO DE TRATAMENTO DE DADO PESSOAL, POR EXEMPLO: CADASTRO DE CLIENTE

Qual a **NECESSIDADE** e a **FINALIDADE**. Tenho **necessidade** de todos estes dados para alcançar esta **finalidade**?

TRANSPARÊNCIA: Como avisamos o titular sobre a coleta dos dados para esta **finalidade**?

Estou fazendo isso com **SEGURANÇA**? Adotando medidas de **prevenção** de danos ao titular?

ADEQUAÇÃO: Os dados que eu processo são adequados para o alcance da finalidade informada?

LIVRE ACESSO: garantia ao titular de consulta facilitada e gratuita sobre a forma e a duração do tratamento

NÃO DISCRIMINAÇÃO: impossibilidade de realização de tratamento para fins discriminatórios, ilícitos ou abusivos.

QUALIDADE DOS DADOS: garantir ao titular exatidão, clareza relevância e atualização de seus dados

Responsabilização e prestação de contas

3. Verificação/ aplicação da base legal (ref. Imagem número 3).

O Tratamento de Dados Pessoais deve sempre ter uma base legal que o legitime. As bases legais estão descritas nos artigos 7 (Dados pessoais) e 11 (dados pessoais sensíveis) da LGPD.

4. Atividades que acarretem risco (ref. Imagem número 4)

É recomendável que para os Tratamentos que acarretem riscos aos Titulares de dados seja realizada uma análise de risco. Essa análise de risco ainda não é regulada, mas poderá vir a ser solicitada pela ANPD. Apesar de não existir recomendação expressa na LGPD sobre o assunto, sempre que o Tratamento de Dados Pessoais for baseado no legítimo interesse, é recomendável que se realize uma análise de balanceamento entre os direitos dos Titulares de Dados e a intenção da BTS de usar os seus Dados Pessoais.

5. Privacy by Design e by Default (ref. Imagem número 5)

É recomendável sempre que houver um Novo Processo de Tratamento, que as normas de proteção de dados sejam aplicadas desde o início da formulação deste processo até o seu final.

6. Aviso de transparência (ref. Imagem número 6)

O Titular tem direito ao acesso facilitado as informações sobre o Tratamento de seus Dados Pessoais, que deverão ser disponibilizadas de forma clara, adequada e ostensiva. O aviso/política de privacidade, deve conter todas as informações constantes no artigo 9º da LGPD. Vislumbra-se, assim, a necessidade de manter o mapeamento de dados atualizado, de forma a garantir que as informações constantes do Aviso/Política de Privacidade estejam atualizadas.

- Qualificação da BTS e os dados para contato;
- Contato e identificação do Encarregado;
- As finalidades específicas do Tratamento;
- Forma e duração de Tratamento;
- Terceiros com os quais a BTS compartilha os Dados Pessoais; e
- Informação sobre a transferência de Dados Pessoais para outro país.
- Responsabilidades dos agentes que realizarão o tratamento
- Direitos do titular.

7. Transferências Internacionais (ref. Imagem número 7)

Os Dados Pessoais apenas podem ser transferidos internacionalmente se a BTS implementar ferramentas jurídicas e/ou organizacionais, por meio de

documentos e/ou códigos de conduta e/ou normas corporativas globais, para viabilizar essa transferência.

8. Ciclo do Dado Pessoal (ref. Imagem número 8)

O processamento dos dados pessoais deve ter um ciclo: coleta, processamento, armazenamento e descarte.

8.1. Diretrizes sobre a coleta e o processamento do dado pessoal:

- Os dados deverão ser coletados para uma **finalidade** específica, que seja devidamente identificada, registrada e comunicada ao Titular;
- Os dados coletados serão sempre aqueles estritamente **necessários** ao cumprimento das finalidades que motivaram sua coleta;
- A coleta de dados só será realizada a partir de fontes fidedignas e, quando feita a partir de Terceiro que não o próprio titular, mediante a formalização das condições contratuais adequadas.
- Os Dados Pessoais coletados pela BTS deverão ser tratados apenas enquanto houver uma finalidade definida e uma base legal aplicável ao Tratamento de tais Dados Pessoais.
- Os Dados Pessoais serão utilizados e manuseados estritamente para as finalidades determinadas quando de sua coleta. Os Dados Pessoais não poderão ser utilizados para finalidades diferentes das originais. Caso haja necessidade de Tratamento de Dados Pessoais para finalidades adicionais às originais, o Encarregado ou responsável pelo tratamento deverá ser consultado
- Apenas os Dados Pessoais que forem necessários para atingir uma finalidade identificada devem ser armazenados. Os Dados Pessoais apenas poderão ser armazenados durante o período estritamente necessário para cumprimento com a finalidade que justificou a sua coleta, a menos que a BTS possua um outro embasamento legal para o seu armazenamento por prazo superior.

8.2. Descarte e expurgo Dados Pessoais

Os Dados Pessoais tratados pela BTS deverão ter uma finalidade definida e registrada, bem como uma base legal que justifique o seu Tratamento. Uma vez que essa finalidade não mais seja aplicável e que não exista outra que justifique o Tratamento desse dado pela BTS, esse deverá ser descartado.

Por exemplo: documentos trabalhistas que a BTS possui a obrigação legal de reter, devem ser armazenados pelo prazo descrito em Lei e mesmo que

algun ex-empregado solicite a exclusão destes dados, a BTS não poderá excluí-los pois possui a obrigação legal de mantê-los. Passado esse prazo legal, se não houver outro motivo para o armazenamento desse dado, esse deve ser descartado.

9. Atendimento aos Direitos dos Titulares. (ref. Imagem número 9)

Para melhor atendimento aos Titulares, recomendamos a implementação de um e-mail destacado para esse assunto na política de privacidade ou mesmo, a implementação de algum sistema que gerencie e documente os atendimentos aos Titulares. Essa demonstração sobre os atendimentos é importante no caso de uma auditoria pela ANPD.

Recomendamos que os Titulares sejam atendidos conforme o manual enviado.

10. Boas Práticas em geral (ref. Imagem número 11)

É recomendável que os Controladores tenham um programa de governança de proteção de dados, bem como Políticas de tratamento de dados para que seus funcionários, Terceiros e demais prestadores que tenham acesso aos dados, saibam como devem manejá-los e quais são as sanções previstas para quem transgredir com tais políticas.

11. Diretrizes sobre gestão de Terceiros (ref. Imagem número 12)

Pela LGPD, o Operador deve seguir as regras do Controlador sobre processamento de dados e caso as descumpra, responderá por este Tratamento. Desta forma, recomenda-se que seja firmado com os operadores de dados, cláusulas específicas de proteção de dados. A BTS deverá determinar e informar à Operadores de Dados Pessoais a finalidade designada para o Tratamento de Dados Pessoais realizado por esse.

12. Segurança da Informação (Ref imagem 12 e 14)

Não há como se falar em proteção de dados, sem que tenha medidas eficazes de segurança da informação. Desta forma, recomenda-se que a BTS adote medidas de segurança, técnicas e administrativas, aptas a proteger os Dados Pessoais sob sua responsabilidade de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado ou ilícito.

As medidas de segurança devem estar aplicadas e serem passíveis de demonstração. Também é recomendável neste sentido, uma política de segurança da informação, com as regras aplicáveis à segurança da informação pela BTS.

13. Plano de Resposta a Incidentes de Segurança (Ref imagem 13 e 14)

Um Incidente de Segurança consiste em um evento ou conjunto de circunstâncias que cause ou possa causar danos ou de qualquer forma prejudicar a disponibilidade, confidencialidade e integridade dos Dados Pessoais contidos ou de qualquer forma derivados das informações, sistemas e operações da BTS. Incidentes de segurança podem afetar Dados Pessoais relacionados a clientes, colaboradores e quaisquer Terceiros que sejam Titulares de Dados Pessoais objeto de Tratamento pela BTS. Exemplos de incidente de segurança incluem exposição de contratos contendo qualificação das partes, divulgação indevida de dados de usuários que postam em redes sociais de clientes, prontuários de saúde de colaboradores da BTS, imagens de câmeras de segurança, exclusão acidental de listas de clientes que incluam dados de pessoas físicas, dentre outros.

Como boa prática temos que as empresas devem manter um registro dos incidentes sofridos, ainda, devem ter um plano de mitigação, bem como medidas de prevenção para que esses incidentes não ocorram mais.

Quando o Incidente causar grande risco ao titular de dados, a BTS deverá comunicar à ANPD (em formulário próprio da ANPD) em até 2 dias úteis. Para tanto, é imprescindível que a BTS tenha um plano de resposta à incidentes, que a habilite a identificar o incidente, mitigá-lo, notificar aos titulares sobre possíveis danos e ainda, responder tempestivamente à ANPD.

14. Treinamentos (ref imagem: 11 e 14)

Treinamentos devem ser realizados para conscientizar as pessoas que trabalham para BTS sobre a importância da proteção de Dados Pessoais. Através dos treinamentos os colaboradores da BTS podem entender o que é um incidente de segurança, como se prevenir, como comunicar um incidente, como agir com novas atividades de tratamento, para qual canal encaminhar solicitações de Titulares, etc.

Os treinamentos são usados para demonstrar que a empresa fez sua parte ao sofrer um incidente de segurança e pode abrandas autuações pela ANPD.

ANEXO I
Modelo simples de Inventário de Dados

RESPONSÁVEL	DESCRIÇÃO DO TRATAMENTO						COMPARTILHAMENTO E TRANSFERÊNCIAS INTERNACIONAIS							
Área	Finalidade do Tratamento	Atividade Primária (Processo)	Atividades secundárias (Detalhamento)	Dados pessoais envolvidos	Titular dos dados	Base Legal do Tratamento	Forma de coleta	Tipo do dado	Compartilha com terceiros?	Qual a finalidade do compartilhamento com terceiro?	Os Dados Pessoais são transferidos para fora do território brasileiro?	Transferência internacional baseada em contrato formalizado?	País/Países para os quais os dados são transferidos?	Prazo de retenção
Operações	Criação de conta de usuário	Cadastro de novos usuários	Cadastro realizado por meio do app	Nome, e-mail, endereço completo	Clientes		Fornecimento pelo titular	Digital	Sim	Armazenamento AWS	Não	Sim	Estados Unidos	Não há

ANEXO II

Modelo de cláusula contratual padrão sobre proteção de dados pessoais para utilização em propostas comerciais e contratos com clientes.

Cláusula para constar em orçamentos e propostas.

"A BTS usará as informações e eventuais dados pessoais contidos nos documentos ou enviados diretamente pelo Cliente para prestação dos serviços de tradução, para saber mais, por favor, consulte nossa Política de privacidade em "link"

Cláusulas para constar em contratos:

Durante a prestação de tradução de serviços linguísticos, a BTS poderá receber dados de clientes relativos a cadastro ou mesmo dados contidos nos próprios documentos alvo das traduções. Para tanto, a BTS tratará os Dados Pessoais de acordo as leis e regulamentos de proteção de dados pessoais aplicáveis e apenas para execução do Contrato, exceto nos casos em que o Tratamento seja necessário para o cumprimento de obrigações legais ou regulatórias a que se sujeitem as Partes.