PROPOSTA DE MODIFICAÇÃO DA MINUTA DE RESOLUÇÃO XXX DE 2021

Regulamenta a aplicação da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD),com base nas competências previstas no art. 55-J, inciso XVIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XVIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da ANPD, tendo em vista a deliberação tomada em sua Reunião Deliberativa nº xxxx, realizada em xx de xxx de 2021 e pelo que consta no processo 00261.000054/2021-37,

RESOLVE:

TÍTULO I
DISPOSIÇÕES GERAIS

CAPÍTULO I
DISPOSIÇÕESPRELIMINARES

Art. 1º Esta resolução regulamenta a aplicação da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:

I - microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966, da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e § 4º [1] da Lei Complementar nº 123, de 14 de dezembro de 2006;

II – *startups*: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no art. 3º e § 4º da Lei Complementar nº 123, de 14 de dezembro de 2006 [2] ~~§ 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021;~~[3]

1 – O Artigo 3º §4º da LC 123/2006 deixa expresso que as espécies empresariais mencionadas não poderão se beneficiar do tratamento jurídico diferenciado previsto nesta Lei Complementar, incluído o regime de que trata o art. 12 desta Lei Complementar, para nenhum efeito legal, a pessoa jurídica mencionada nos incisos I ao XI;

2 – O Artigo 3º §4º da LC 123/2021 deixa expreesso que as startups não poderão se beneficiar do tratamento jurídico diferenciado previsto nesta Lei Complementar, incluído o regime de que trata o art. 12 desta Lei Complementar, para nenhum efeito legal, a pessoa jurídica mencionada nos incisos I ao XI;

3 – O §1º do art. 4º da LC 182/2021 faz referência ao enquadramento na modalidade de tratamento especial destinada a fomento para as startups, o que não se confunde com isenção para o cumprimento, mesmo que flexível, da Lei 13.709/2018;

III ~~– pessoas jurídicas sem fins lucrativos: associações, fundações, organizações religiosas e partidos políticos;~~ [4]

IV – agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

V – zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.

~~Parágrafo único. Para fins desta resolução, consideram-se, ainda, agentes de tratamento de pequeno porte, os que possuem receita bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.~~[5]

Art. 3º A ~~dispensa e a~~ [6] flexibilização das obrigações previstas nesta resolução não são aplicáveis a agentes de tratamento de pequeno porte que realizem tratamento de alto risco e em larga escala para os titulares. ~~ressalvada a hipótese prevista no art. 13, Parágrafo único,~~ [7]

I – A determinação de larga escala, sob a consideração de extensão geográfica, dar-se-á na medida do número proporcional de titulares, sob tratamento pelo agente, for igual ou superior a 5% (cinco por cento) da população atendida pelo agente, seja territorialmente considerado Município, Estado ou todo o Território Nacional, a depender da extenção do alcance de sua atividade empresarial, conforme censo mais recente e poderá ser determinada ainda, de acordo com levantamento ou ação fiscalizatória da própria autoridade. [8]

II – Para os fins do inciso I, do art. 3°, considera-se atuação de extensão geográfica municpal, empresas que atuem em até 4 municípios, a partir deste número considera-se a extensão georgráfica estadual e, a partir da atuação em mais de 3 estados, considera-se a extensão geográfica de todo o território nacional.

§ 1º Para fins desta resolução, será considerado tratamento de alto risco para aos titulares, ~~entre outras hipóteses~~, [9] o tratamento que envolva:

I - dados sensíveis conforme Lei 13.709, de 14 de agosto de 2018 artigo 5°, incido II ou dados de grupos vulneráveis, incluindo crianças, adolescentes e idosos, considerados conforme a natureza jurídica dispostas na Lei 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente – ECA) e Lei 10.741, de 01 de outubro de 2003 (Estatuto do Idoso);

Il – vigilância ou controle de zonas acessíveis ao público;

Ill – uso de tecnologias emergentes, que possam ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; ou

IV – tratamento automatizado de dados pessoais que afetem os interesses dos titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 2º O tratamento de dados será caracterizado como de larga escala quando abranger número significativo de titulares, conforme inciso I, do artigo 3° desta Regulamentação, considerando-se, ainda, o volume de dados envolvidos, bem como a duração e a frequência. ~~e a extensão geográfica do tratamento realizado~~.[10]

---

4 – Fere os direitos dos titulares de dados dos grupos mencionados, de acordo com os artigos 5º, "caput", II, X, e XXXV, 37 e 84, IV da Constituição Federal; Artigo 2º, II, IV, VI e VII da lei nº 13.709/2018; registre-se que, os dados de opção sindical, política e crença religiosa por si só já são considerados sensíveis à luz da LGPD, a necessitar de tratamento especial e não de flexibilização;

5 – O referido parágrafo único não deve levar somente como parâmetro a receita bruta anual das EPPs e MEs para fins de flexibilização, uma vez que inobserva o volume e o fluxo dos dados dos titulares e em total desacordo com os princípios da legalidade, impessoalidade e eficiência dos atos administrativos; Esse P. Único contraria a Lei complementar 123/2006 (art.3, pra. 4), que definie EPP;

6 – A palavra “dispensa” deve ser retirada, uma vez que, de acordo com os princípios que regem a atividade legislativa, bem como da hierarquida das normas, não é de competencia da minuta criar ou extinguir direitos, nos moldes do art. 5º, XXXVI da Constituição Federal;

7 – O constante no o Art. 13, § único da Lei 13.709/2018 não o isenta o contrtolador de pequeno porte de ter os mesmos cuidados técnicos que um encarregado teria, de modo que, se faz prudente uma contratação flexível desta especie de profissional, respeitando o caput do art. 170 da CF que trata da ordem econômica e financeira, em especial no príncípio da funçao social da propriedade e defesa do consumidor , bem como o artigo 2º, V da Lei 13.709/2018 que tutela o desenvolvimento econônico dos PMEs. Ademais, as flexibilizações não alcançam os agentes de pequeno porte que tratam dados em larga escala e alto risco, portanto, descabe a manutenção da ressalva posta quanto ao Encarregado;

8 – Tal parametrização se baseia no Direito comparado à Alemanha e Estônia, guardadas as devidas proporções;

9 – Critério subjetivo que dá margem à discussão e traz insegurança jurídica nas relações;

10 – O termo “extensão geográfica” desacompanhado de qualquer outro parâmetro gera ambiguidades, podendo causar inúmeras interpretações equivocadas da lei;

~~§ 3º Para fins deste artigo não será considerado tratamento de larga escala o tratamento de dados de funcionários ou para fins exclusivos de gestão administrativa do agente de tratamento de pequeno porte.~~[11]

~~§ 4º A ANPD disponibilizará guias e orientações que auxiliem os agentes de tratamento de pequeno porte a avaliar se realizam tratamento com alto risco e em larga escala.~~[12]

Art. 4º Caberá ao agente de tratamento de pequeno porte avaliar e, quando solicitado pela ANPD, comprovar o seu enquadramento nas disposições do art. 2º e do art. 3º.

Parágrafo único. A ANPD poderá alterar o enquadramento apresentado pelo agente de tratamento de pequeno porte em sua atividade fiscalizatória.

TÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS PELOS AGENTES DE TRATAMENTO DE PEQUENO PORTE

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 5º A ~~dispensa ou~~ [13] flexibilização das obrigações dispostas nesta resolução não isenta, em qualquer caso, os agentes de tratamento de pequeno porte do cumprimento de outras disposições legais e regulamentares relativas à proteção de dados pessoais.

CAPÍTULO II
DAS OBRIGAÇÕES DO AGENTE DE TRATAMENTO DE PEQUENO PORTE

Seção I
Das obrigações relacionadas aos direitos do titular

Art. 6º Os agentes de tratamento de pequeno porte devem ~~podem~~ [14] atender às requisições dos titulares de dados pessoais, descritas no art. 18, da LGPD, por meio eletrônico ou impresso.

~~§1º Os agentes de tratamento de pequeno porte estão dispensados de conferir portabilidade dos dados do titular a outro fornecedor de serviço ou produto, nos termos do inciso V do art. 18 da LGPD.~~ [15]

~~§2º É facultado ao agente de tratamento de pequeno porte, quando solicitado pelo titular de dados, optar entre anonimizar, bloquear ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, na forma do art. 18, inciso IV, da LGPD.~~[16]

~~Art. 7º Os agentes de tratamento de pequeno porte ficam dispensados de fornecer a declaração clara e completa de que trata o art. 19, inciso II, da LGPD.~~[17]

Art. 8º A disponibilização das informações sobre o tratamento de dados pessoais, nos termos do art. 9º, da LGPD, pode ocorrer por meio eletrônico ou por qualquer outra forma que assegure o acesso facilitado e gratuito [18] às informações pelo titular dos dados pessoais.

~~Art. 9º Fica facultado aos agentes de tratamento de pequeno porte, inclusive àqueles que realizam tratamento de alto risco e em larga escala, fazerem-se representar por entidades de representação da atividade empresarial, por pessoas jurídicas ou por pessoas naturais para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares de dados.~~

~~Parágrafo único. A assessoria também poderá ser prestada por pessoas jurídicas sem fins lucrativos e pessoas naturais.~~ [19]

---

11 – A dispensa para tratamento dos dados de funcionários fere o princípio da isonomia, uma vez que os mesmo são títulares de dados, conforme preceituam os artigos 5º, "caput", II, X, e XXXV, 37 e 84, IV da Constituição Federal; Artigo 2º, II, IV, VI e VII da lei nº 13.709/2018;

12 – O objetivo da minuta é regulamentar a aplicação da Lei 13.709/2018, e, neste momento, estabelecer os parâmetros necessários do que venham a ser alto risco e larga escala para auxiliar os agentes de tratamento de pegueno porte nesta avaliação. Postergar tais definições *a posteriori* viola o princípio da eficiência dos atos administrativos, uma vez que não se pode falar em eficiência sem falar em planejamento, não existindo previsão legal de regulamentação de regulamentação, portanto, nula de pleno direito;

13 - A palavra “dispensa” deve ser retirada, uma vez que de acordo com a os princípios que regem a atividade legislativa, bem como da hierarquida das normas, não é de competencia da minuta criar ou extinguir direitos, nos moldes do art. 5º, XXXVI da Constituição Federal; trata-se de nulidade, passível de discussão de sua validade jurídica na medida em que uma Resolução não pode alterar a Lei Geral vigente;

14 – Não se trata de uma faculdade ao controlador em atender as requisições dos titulares de dados e sim uma obrigação, uma vez que de acordo com o art. 2º,VII, 6º, IV, VI e 9º da Lei 13.709/2018 tais requisições são um direito do titular do dados;

15 – Dispensar o agente de tratamento de conferir portabilidade dos dados pessoais do titular a outro fornecedor de produto ou serviço exclui direitos e garantias fundamentais deste segundo, uma vez que os dados são do titular, de acordo com o artigos 1º e 9º, § 3º da Lei 13.709/2018;

16 – Dar este tipo de faculdade ao agente de tratamento exclui os direitos e garantias fundamentais do titular de dados, uma vez que de acordo com os artigos 1º, 2º IV, V e VI; 6º I, IV, V, VI e X; 9º, §3º da Lei 13.709/2018 tais dados são do titular e é um direito do mesmo ter a suas solicitações atendidas;

17 – Seguem os mesmos critérios de inaplicabilidade do artigo 6º, §§ 1º e 2º desta minuta;

18 – A disponibilização destas informações devem ser gratuitas, de acordo com o principio do Livre Acesso, insculpido no artigo 6º, IV da LGPD;

19 - A possibilidade dos agentes de tratamento de pequeno porte serem representados por entidades é uma flexibilização que, por sua vez, cria direitos, o que é ilegal para uma regulamentação, conforme já disposto anteriormente, além de criar uma reserva de mercado às federações, associações e sindicatos de representação de categorias, uma vez que a Lei 13.709/2018 já prevê a modalidade de prestação de serviço de Encarregado pelo Tratamento de Dados Pessoais como serviço;

Seção II
Do Registro das Atividades de Tratamento

~~Art. 10. Os agentes de tratamento de pequeno porte ficam dispensados da obrigação de manutenção de registros das operações de tratamento de dados pessoais constante do art. 37 da LGPD.~~ [20]

~~Parágrafo único.~~ A ANPD, no anexo I, ~~fornecerá~~ apresenta modelos para o registro ~~voluntário e~~ [21] simplificado das atividades de tratamento por agentes de tratamento de pequeno porte~~,~~ e considerará a existência de tais registros para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.

Seção III
Do Relatório de Impacto à Proteção de Dados Pessoais

Art. 11. Os agentes de tratamento de pequeno porte podem [22] apresentar o relatório de impacto à proteção de dados pessoais, quando solicitado pela ANPD, de forma simplificada, nos termos do artigo 38, parágrafo único, da LGPD, conforme anexo II. ~~quando for exigido, nos termos da resolução específica.~~

Seção IV
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 13. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41, da LGPD, sendo de sua inteira responsabilidade os eventuais incidentes decorrentes da falta de nomeação deste;

Parágrafo único. O agente de tratamento de pequeno porte, que não indicar um encarregado, deve disponibilizar um canal de comunicação com o titular de dados, cujo atendimento deve ser feito por profissional com profundo conhecimento sobre a legislação de proteção de dados. [24]

Seção VI
Da Segurança e das Boas Práticas

Art. 14. Os agentes de tratamento de pequeno porte ~~devem adotar medidas administrativas e técnicas essenciais e necessárias, com base nos requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando,~~ devem adotar medidas de segurança, técnicas e administrativas, com base em requisitos mínimos de segurança da informação, para proteção dos dados pessoais, previstos no anexo IV, desta Resolução, conforme as regras de segurança das normas da ABNT, NBR, ISO, IEC. ~~, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.~~ [25]

~~Parágrafo único. A ANPD disponibilizará guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.~~[26]

~~Art. 15. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.~~[27]

---

20 – Não se pode dispensar ao agente de tratamento de pequeno porte a manutenção do registro das operações de tratamento dos dados pessoais dos titulares, por violar o disposto nos artigos 1º, 2º IV, V e VI; 6º I, IV, V, VI e X; 9º, §3º da Lei 13.709/2018, bem como o próprio artigo 37, LGPD que dispõe expressamente “que devem ser mantidos os registros” e a Regulamentação não pode restringir direitos, especialmente quando baseados no legítimo interesse que é uma das hipóteses de tratamento de dados pessoais com maior precoupação pelo legislação que criou, diversos requisitos a serem, obrigatoriamente, cumpridos, razão pela qual torna o referido artigo 10 da minuta ilegal;

21 – A apresentação do registro das atividades de tratamento dos dados pessoais dos titulares não é uma mera faculdade por parte destes agentes de tratamento, ainda que de forma simplificada, motivo pelo qual tal modelo voluntário deve inexistir por parte da ANPD, uma vez que a autoridade fiscalizadora não detém competência para dispensa deste, pois estaria violando o princípio da isonomia disposto no art. 5º, "caput", II, X, e XXXV, 37 e 84, IV da CF, bem como o princípio da impessoalidade no direito administrativo, conforme Lei 9784/1999, assim o modelo apressentado na sugestão do Anexo I, deve ser simplificado, nao voluntário;

22 – Deve-se flexibilizar ao agente de tratamento de pequeno porte que tal registro seja de forma simplificada, em respeito aos caput do art. 170, da CF, que trata da ordem econômica e financeira; bem como o artigo 2º, inciso V, da Lei 13.709/2018, que tutela o desenvolvimento econômico das PMEs, em cumprimento ao artigo 38, em seu parágrado único, da LGPD, quando solicitado pela ANPD;

23 – Seguem os mesmos critérios de aplicação do art. 3º desta minuta, ora retificada;

24 – O que se visa é a garantia dos direitos do titular, sobretudo no que dispõe o artigo 6º, IV, V e VI da LGPD;

25 – O artigo 14 da minuta deve-se pautar em critérios técnicos já reconhecidos e amplamente utilizados, à exemplo das normas ABNT, NBR, ISO, IEC;

26 – A ANPD, no anexo IV, dispõe de Política de Segurança da Informação e Boas Práticas simplificadas, utilizando parâmetros já reconhecidos internacionamente contidos nas normas da ABNT NBR ISO/IEC;

27 – O s Artigos 14 e 15 devem ir de acordo com as normas NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, 2013), baseada na norma BS 7799 (British Standard), que já tem definidos os parâmetros técnicos e cientificos.

Art. 15. Os agentes de tratamento de pequeno porte devem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme o anexo IV, desta Resolução.[28]

~~§1º A política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte, bem como a sensibilidade e a criticidade dos dados tratados diante dos direitos e liberdades do titular.~~ [29]

§2º A ANPD considerará a existência das políticas simplificadas de segurança da informação para fins do disposto no art. 6º, inciso X e no art. 52, §1º, incisos VIII e IX da LGPD.

TÍTULO IV
DOS PRAZOS DIFERENCIADOS

Art. 16. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:

I – no atendimento das solicitações dos titulares, referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, parágrafos 3º e 5º, da LGPD; ~~nos termos da resolução específica~~ [30];

II – na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, ~~nos termos da resolução específica~~ [31], exceto quando houver potencial comprometimento à integridade dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento ~~conforme os termos da mencionada resolução~~;

III – em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

Parágrafo único. Os prazos não especificados nesta resolução para agentes de tratamento de pequeno porte ~~serão determinados por resoluções específicas.~~[32] seguem os dispositivos da LGPD.

TÍTULO V
DISPOSIÇÕES FINAIS

Art. 17. A ANPD disponibiliza, ~~divulgará~~ nesta resolução, anexos com documentos simplificados para os agentes de tratamento de pequeno porte ~~guias orientativos de aplicação da LGPD para agentes de tratamento de pequeno porte~~.[33]

~~Art. 18. Resoluções específicas poderão dispor sobre outras normas de tratamento simplificado a agentes de tratamento de pequeno porte.~~[34]

~~Art. 19. A ANPD poderá determinar ao agente de tratamento de pequeno porte o cumprimento de obrigações dispensadas ou~~ [35] ~~flexibilizadas nesta Resolução, considerando as circunstâncias relevantes da situação, tais como a natureza e o volume das operações, os riscos para os titulares e a sensibilidade e a criticidade dosdados tratados.~~

~~Parágrafo único. A decisão de que trata o caput será motivada, assegurado o direito ao contraditório e à ampla defesa~~ [36]

Art. 20 Esta resolução entra em vigor no dia 1º de XXXXX de XXXX.

---

28 – O s Artigos 14 e 15 devem ir de acordo com as normas NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, 2013), baseada na norma BS 7799 (British Standard), que já tem definidos os parâmetros técnicos e cientificos, e, desta feita, segue anexo IV com as devidas pontuações;
29 – segue os mesmos critérios do artigo 15 ora retificado;
30 – Resolução para uma resolução é atécnico e em dissonancia com o princípio da eficiência dos atos administrativos, conforme lei 9784/1999;
31 – Não pode a ANPD, nesta resolução, abrir margem para uma nova resolução por meio desta espécie de lacuna, uma vez que tal materia como já fartamente demonstrada deve ir de acordo com as normas NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, 2013), baseada na norma BS 7799 (British Standard), que já tem definidos os parâmetros técnicos e cientificos, ou seja, a minuta não pode inovar o que já existe, ferindo o princípio da legalidade e eficiência dos atos administrativos;
32 – Não cabe a ANPD a edição de novas resoluções específicas acerca dos prazos, uma vez que o própro artigo 16 desta minuta já estabelece-os, e, em sua omissão vigora a própria LGPD;
33 – Resolução para uma resolução é atécnico e em dissonancia com o princípio da eficiência dos atos administrativos;
34 – A palavra “dispensadas” deve ser retirada, uma vez que de acordo com a os princípios que regem a atividade legislativa, bem como da hierarquida das normas, não é de competencia da minuta criar ou extinguir direitos, nos moldes do art. 5º, XXXVI da Constituição Federal, bem como o artigo 55-J, inciso XVIII, da Lei 13.709/2018;
35 – Toda e qualquer norma de cunho técnico e cientifico que vise a proteção de dados pessoais por parte dos controladores de pequeno porte devem observar as regras já estabelecidas e amplamente utilizadas, de acordo com as normas NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, 2013), baseada na norma BS 7799 (British Standard), que já tem definidos tais parâmetros;
36 - Seguem os mesmos critérios de aplicação do art. 19 desta minuta, ora retificada.

ANEXO I

Modelo Simplificado de Relatório de Registro de

Operações de Tratamento de Dados Pessoais

(inclusive quando a hipótese de tratamento for o Legítimo Interesse):

Artigo 37, Lei 13.709/2018

Controlador: Razão Social/Nome e CNPJ/CPF:							
Dados para contato:							
Período do tratamento informado: De				à			
Categoria dos Dados Tratados:							
Dados comuns		Dados sensíveis					
Alegou hipótese de tratamento de Legítimo Interesse?							
Sim		Não					
Tipos de Dados tratados:							
Registro Geral – RG		Cadastro de Pessoa Física - CPF					
Nome		Carteira Nacional de Habilitação - CNH					
Endereço		E-mail					
Telefone e/ou celular		Data de nascimento					
Programa de Integração Social – PIS		Título de eleitor					
Carteira de Trabalho e Previdência Social – CTPS		Dados de ascendentes e/ou dependentes					
Outros, descreva:		Se tratar dados sensíveis, indicar quais:					
Agente de tratamento dos dados:							
Controlador		Operador:					
Caso hajam operadores envolvidos, indique o nome/razão social e o CPF/CNPJ dos mesmos:							
Finalidade do Tratamento:							

Hipótese de Tratamento dos Dados conforme artigos 7° e 11, da Lei Geral de Proteção de Dados:					
Consentimento		*Artigo 7, I*		*Artigo 11, I*	
Obrigação Legal		*Artigo 7, II*		*Artigo 11, II.a*	
Administração Pública		*Artigo 7, III*		*Artigo 11, II.b*	
Realização de estudos		*Artigo 7, IV*		*Artigo 11, II.c*	
Execução de contrato		*Artigo 7, V*		*Artigo 11, II.d*	
Para exercício regular do direito		*Artigo 7, VI*		*Artigo 11, II.d*	
Para proteção da vida		*Artigo 7, VII*		*Artigo 11, II,e*	
Para tutela de Saúde		*Artigo 7, VIII*		*Artigo 11, II.f*	
Interesse legítimo do controlador		*Artigo 7, IX*			
Para proteção ao crédito		*Artigo 7, X*			

Data:

ANEXO II

Modelo Simplificado de Relatório de Impacto à Proteção de Dados

(inclusive quando a hipótese de tratamento for o Legítimo Interesse):

Art. 5°, inciso XVII, LGPD, Lei 13.709/2018

Controlador: Razão Social/Nome e CNPJ/CPF:

Dados para contato:

Operadores: Indicar os nomes ou razões sociais, CNPJ/CPF e contato:

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos 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.

Tratamento de dados pessoais:

1) Finalidade: descreva o escopo do tratamento

2) Hipótese de tratamento: Indique dentro dos artigos 7° e 11 , quais as hipóteses de tratamento específicas

Consentimento		*Artigo 7, I*		*Artigo 11, I*	
Obrigação Legal		*Artigo 7, II*		*Artigo 11, II.a*	
Administração Pública		*Artigo 7, III*		*Artigo 11, II.b*	
Realização de estudos		*Artigo 7, IV*		*Artigo 11, II.c*	
Execução de contrato		*Artigo 7, V*		*Artigo 11, II.d*	
Para exercício regular do direito		*Artigo 7, VI*		*Artigo 11, II.d*	
Para proteção da vida		*Artigo 7, VII*		*Artigo 11, II,e*	
Para tutela de Saúde		*Artigo 7, VIII*		*Artigo 11, II.f*	
Interesse legítimo do controlador		*Artigo 7, IX*			
Para proteção ao crédito		*Artigo 7, X*			

3) Tipo dos dados:

Dados comuns		Dados sensíveis	
Dados que podem gerar riscos às liberdades civis ou aos direitos fundamentais			

4) Riscos envolvidos:

Para o preenchimento, considere a formula probabilidade versus impacto, siga o modelo da tabela abaixo

Probabilidade (P)				
	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
	Impacto (I)			

ID	Risco referente ao tratamento de dados pessoais	P	I	Nível de risco (P x I)
R01	**Acesso fisico não autorizado. (Exemplo de preenchimento)**	**10**	**15**	**150**

5) Grau de risco:

Baixo		Moderado		Alto	

6) Protocolo de mitigação/prevenção:

Contato com os titulares		Troca periódica de senhas	
Cópia de segurança: Data da ultima cópia:		Teste de cópia de segurança: Qual a periodicidade:	
Treinamentos		Anti-virus e proteçãod e rede: Quais?	
Existe controle de acesso ao centro de processamento de dados - CPD		Existe controle de acesso ao sistema	
Existe arquivos fisicos:		Existe controle de acesso aos arquivos fisicos:	
Sistema operacional, atualiado: Qual:		Existe aplicativo ou sistema sem a devida liceça do fornecedor:	
O sistema de gestão da empresa é interno (servidor fisico) ou em nuvem:		Se o sistema for em nuvem, qual o fornecedor:	
Existe acesso remoto de funcionários ou operadores, via rede privada (teletrabalho)		Se em nuvem, qual a forma de segurança para o acesso:	
È feito teste de vulnerabilidades, data do ultimo teste:		O Sistema tem duplo fator de autenticação:	

Data:

ANEXO III

Modelo Simplificado de Comunicação de Incidente de Segurança

Artigo 38, parágrafo único, LGPD, Lei 13.709/2018

Controlador: Razão Social/Nome e CNPJ/CPF:					
Dados para contato:					
Operadores: Indicar os nomes ou razões sociais, CNPJ/CPF e contato:					
1) Data do incidente de segurança:					
2) Hora do incidente:					
3) Tipo de incidente Digital					
Interno* – dentro da organização e/ou operadores (acesso indevido)					
Externo** – compartilhamento indevido					
Vazamento de dados		Implicito***		Explicito****	
Ataque cibernético, utiliando engenharia social					
Ataque cibernético direto					
Em apuração					
Outros: descreva abaixo					
4) Tipo de incidente fisico ou analógico					
Interno* – dentro da organização e/ou operadores (acesso indevido)					
Externo** – compartilhamento indevido					
Vazamento de dados		Implicito***		Explicito****	
Ataque utiliando engenharia social					
Em apuração					
Outros: descreva abaixo					
*Interno: ação ou omissão de um funcionário ou contratado da organização;					
** Externo: agente de origem externa alheio à organização;					

*** Implícito: a organização não tem conhecimento se os dados pessoais, sob seu controle foram expostos; **** Explícito: a organização tem conhecimento que os dados pessoais, sob seu controle, foram expostos.
5) Descreva os detalhes conhecidos do Incidente de Segurança até o momento desta informação:

6) Número de titulares afetados:	

7) Tipos de dados afetados:

Nome		RG	
CPF		Endereço	
E-mail		Telefone e/ou celular	
Data de Nascimento		PIS	
Titulo de eleitor		CTPS	
Dados de Ascendentes e/ou dependentes		Outros, descreva nas linhas abaixo:	

8) Medidas de Salvaguarda anteriores ao incidente de segurança:

Licenças de programas e apps em dia		Utilizava antivírus, especifique:	
Tinha firewall, Qual:		Havia backups atualizados, data da última atualização: __/__/___.	
Equipe passou por treinamentos de boas práticas		Havia, mesmo que seja facultativo, Encarregado pelo Tratamento de Dados Pessoais? Em caso positivo, informe o nome e meio de contato:	
Cadeados		Segurança de câmeras internas e externas:	
Sistema de vigilância		Controle de acesso Físico	
Outro, descreva nas linhas abaixo:			

9) Protocolo pós incidente de segurança:

Informação aos titulares		Solicitação de troca de senhas	
Banco de dados restaurados via backup		O incidente continua ativo? Se sim, descreva os detalhes nas linhas abaixo:	

Outros, descreva nas linhas abaixo:
10) Caso a organização não tenha indicado um Encarregado pelo Tratamento de Dados Pessoais, informe quem será o responsável pela comunicação entre a ANPD e a organização:
Data:

ANEXO IV

Modelo Simplificado de Política de Segurança da Informação e Boas Práticas

I - OBJETIVO

Esta Política estabelece os conceitos e diretrizes de segurança da informação, visando proteger as informações da "**EMPRESA**", e de seus clientes. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação da **EMPRESA**. Assim, deve ser entendida como uma declaração formal da Alta Administração acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os funcionários, estagiários e colaboradores terceirizados da **EMPRESA**.

II - DEFINIÇÕES

Segurança da Informação – Visa a preservar as propriedades de confidencialidade, integridade, disponibilidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento.

§ A **EMPRESA** é comprometida com a observância da legislação em vigor aplicável, bem como do Estatuto da Companhia e do Código de Ética e Conduta. E para a condução de suas atividades empresariais é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara que possibilite aderência e conformidade.

2.1 Pilares da Segurança da Informação

A segurança da informação é aqui caracterizada pela preservação dos seguintes pilares:

Confidencialidade: A **EMPRESA** visa garantir que o acesso às informações de colaboradores, parceiros e de seus titulares de dados sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;

Integridade: A **EMPRESA** visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados de titulares que estejam sob sua responsabilidade.

Disponibilidade: A **EMPRESA** visa garantir que a informação esteja sempre disponível aos profissionais que de fato possuam o acesso necessário para tal e assegure que os dados estejam disponíveis de acordo com o nível de acordo de serviço contratado pelos titulares.

§ A **EMPRESA** visa garantir a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registros das transações, quando aplicável e alterações realizadas em seus sistemas e aplicações.

III - Aspectos Gerais

- As informações de titulares devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pelo PPPDP – Política de Privacidade e Proteção de Dados Pessoais da **EMPRESA** e das leis vigentes;
- Os dados pessoais devem ser utilizados somente para os fins correspondentes às hipóteses de tratamento para as quais foram coletados;
- Todos os funcionários, estagiários e colaboradores terceirizados devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, sem aviso prévio, e que os registros assim obtidos podem servir de evidência para a aplicação de medidas disciplinares;
- A **EMPRESA** mantém um compromisso com o cliente em adotar técnicas e meios de segurança mais adequados e disponíveis em relação à segurança dos dados trafegados, processados e/ou armazenados na;
- Os funcionários, estagiários e colaboradores terceirizados, quando aplicável, devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações;
- Os dados pessoais devem ser utilizados de forma transparente e apenas para a finalidade para a qual foram coletados.

3.2 Tratamento da Informação

Para assegurar a proteção adequada aos dados pessoais coletados pela **EMPRESA**, deve existir um método de classificação e rotulagem dos mesmos, de acordo com o grau de confidencialidade e criticidade para os negócios da **EMPRESA**.

§ A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada, de modo a respeitar a intimidade, vida privada, honra e imagem dos titulares.

3.3 Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

Os riscos devem ser identificados por meio de um processo estabelecido para Avaliação dos Riscos de Segurança da Informação simplificados, conforme Anexo II dessa regulamentação.

Os incidentes de Segurança da Informação devem ser analisados, tratados, registrados, monitorados e reportados conforme Anexo III dessa regulamentação.

3.4 Treinamentos de Conscientização

A **EMPRESA** deve realizar treinamentos de forma regular e periódica, de conscientização sobre a Lei Geral de Proteção de Dados, em especial à Segurança da Informação.

§ Cabe à **EMPRESA** promover a divulgação e revisão desta Política para todos os funcionários, estagiários e colaboradores terceirizados.

3.5 Responsabilidades

- De forma geral, cabe a todos os funcionários, estagiários e colaboradores terceirizados cumprir fielmente esta política, sob pena de responsabilização de eventuais danos causados à **EMPRESA** e/ou aos titulares de dados pessoais, conforme dispositivo do Código Civil brasileiro, observadas outras disposições legais;

- Direcionar ocorrências aos responsáveis para que sejam tomadas as devidas providências;

4 Disposições Gerais

Para fins dessa política aconselha-se, adicionalmente, em observação às boas práticas os seguintes parâmetros contidos às normas da família ISO 27000, conforme sugestões abaixo:

1 - Classificação da informação;

2 - Controle de concessão de informação de autenticação secreta;

3 - Não retirar equipamentos, informações ou softwares sem autorização;

4 - Manutenção correta dos equipamentos;

5 - Direitos de acesso privilegiado sejam restritos e controlados;

6- Perfil de acesso dos usuários;

7 - Procedimentos para o trabalho em áreas seguras;

8 - Controle e restrições de programas utilitários;

9 - Requisitos para acordos com fornecedores relacionados a riscos;

10 - Medidas de segurança para ativos fora da organização;

11 - Controles de criptografia usados em conformidade com todas as leis;

12 - Definição de Responsabilidades;

13 - Análise regular dos proprietários de ativos;

14 - Documentar todos os requisitos legais e contratuais;

15 - Privacidade e Proteção das informações quando aplicável;

16 - Procedimento seguro de entrada no sistema (log-on);

17 - Ativos com respectivos proprietários;

18 - Segurança da Informação considerada no gerenciamento de projetos;

19 - Procedimentos apropriados legais e contratuais;

20 - Funcionários e Terceiros praticando a Segurança da Informação;

21 - Registro e cancelamento de usuários;

22 - Análise de todos os equipamentos de mídias antes do descarte;

23 - Política e medidas em locais de trabalho remoto;

24 - Segregação em redes de informação, usuários e SI;

25 - Proteção total dos registros;

26 - Regras para uso aceitável das informações;

27 - Procedimentos para o tratamento de ativos;

28 - Controle de instalação de Software;

29 - Verificação do Histórico para todos os candidatos a emprego;

30 - Regras e critérios para a instalação de software pelos usuários.

§ Eventuais lacunas da presente Política serão tratadas de acordo com legislação pátria.

INICIATIVA E INFORMAÇÕES SOBRE A PROPOSTA DE MINUTA

Tudo que está grafado e marcado em azul foi adicionado pelo grupo do estudos avançados DPO+, tudo que está grafado em vermelho e riscado era o texto original que foi analisado e está em desconformidade com a legislação pátria ou em desacordo com a Lei de Processos Administrativos que proibe, em sede de regulamentação, criar obrigação ou restringir direitos.

Entenda a ANPD que regulamentar não é criar obrigações ou restringir direitos, a ANPD não é legislador, apenas fiscalizador e, obrigatoriamente, deve, apenas, criar processos e parâmetros.

A presente minuta foi analisada pelo Grupo de Estudos Avançados DPO+ (DPO Mais), devendo ser recebida como contribuição do Grupo de Estudos Avançados DPO+ e da ANPPD.

Coordenação Geral: Dra. Silvia Brunelli do Lago – CEO da SAP Treinamentos proprietária do Treinamento Avançado DPO+, idealizadora e fundadora da ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados.

Assistente de coordenação geral: Prof. Hudson Barbosa, DPO – CEO da empresa DPOAAS.

Participou da Audiência Pública como Presidente da ANPPD: Davis Souza Alves – Membro do CNPD.

Integrantes do Grupo de Estudos Avançados DPO+ que participaram da elaboração dessa minuta (todos membros da ANPPD):

Marco Antonio de Oliveira
Marcelo Gonçalves Leite
Laerte Rodrigues de Moura
Rosângela Aparecida de Almeida Medeiros
Viviane Laporti
Sidney Giovanni Simas
José Victor Brujas Junior
Rosineide Mainardes da Silva Alves
Alex Araujo do Nascimento
Lorena Magalhães Sancho
Andreia Amorim Neder
Elizangela Andrade
Luciana Gianello Takano
Elaine Campos
Carlos Fraga
Aline Sartori
Maria Clara Silva de Oliveira Gonçalves
Maria Oliveira Duarte
Luis Ricardo Nary Such
Ariane Pinto
Sabrina Gil Mantecon
Raquel Lovatti Caetano
Carlos Eduardo Moreno
Joselma Vagner
Luciliane Ribeiro
Jaqueline Cerqueira
Yolanda Araripe Eirado
Isilândia Lins
Valéria Cristina Bosso
Marlete Amorim
Shirley Batista Ragazzi
Maria Jucimária Silva dos Santos
Vera Mara da Silva
Keyra Guzmán

André Luiz de Macêdo Soares
Cleia Ribeiro dos Santos
Adriana Bernardi
Milena Stradiotti
Sandra Mara Moraes
Jane Célia Carlone
Paulo Afonso da Silva
Wallace Azevedo Santiago
Sirleni Brandão Secchim
Maurus Otávio Santos
Sergio Benjamin da Silva
Daniele Santos Teixeira de Castro
Dianiele Rosa de Brito
Miriã Cristina do Rio Alvar Moraes
Ana Jucélia Pieczarka Munaretto
Elaine Cristina da Cunha Melnicky
Marcelo Frassei
Irma Sizue Kato
Leandro dos Santos Borges
Laercio Rodrigues de Queiroz Junior
Nêmora Cristina Gomes Rosa
Eduardo Henrique de Oliveira
Ronaldo Fernandes
Rudimar Onofre
Deize de Fátima Almeida Machado
Maria Rivanete do Nascimento
Marcos Giovani Dapper
Kesley Matias Pirett
Adriana Lopes Costa
Kélen Souza Xavier Von Lohrmann Cruz
Christian Barbosa