Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Fiscalização
Coordenação de Fiscalização

RELATÓRIO DE INSTRUÇÃO Nº 3/2024/FIS/CGF - VERSÃO PÚBLICA

Brasília, data da assinatura.

A versão original deste documento, na modalidade restrita, foi assinada em 23/04/2024.

RELATÓRIO DE INSTRUÇÃO[1]

SUMÁRIO

1. IDENTIFICAÇÃO

1.1. **Nome/razão social do autuado:** Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS), sucessora da Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas do Estado de Pernambuco (SDSCJPVD), que sucedeu a Secretaria de Desenvolvimento Social, Criança e Juventude de Pernambuco (SDSCJ)

1.2. **CPF/CNPJ do autuado:** 08.642.138/0001-04

1.3. **Agente de tratamento:** (X) Controlador ( ) Operador

1.4. **Nome do Encarregado setorial:** Luan Moura Paes Barreto (Portaria Designação encarregado setorial LGPD (SDSCJPVD nº 280, de 24/11/23)[2]

1.5. **Contato da(o) Encarregada(o):** luan.barreto@sdscjpvd.pe.gov.br[3]

2. EMENTA

INCIDENTE DE SEGURANÇA EM ÓRGÃO PÚBLICO. DADOS PESSOAIS, DADOS PESSOAIS SENSÍVEIS E DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES. EXPOSIÇÃO DE DADOS POR ACESSO À BASE DE DADOS EM QUE CONSTAVAM DADOS PESSOAIS UTILIZADOS PARA INSCRIÇÃO EM POLÍTICA PÚBLICA DE TRANSPORTE COLETIVO. NÃO COMUNICAÇÃO AOS TITULARES. AUSÊNCIA DE COMPROVAÇÃO DE ATENDIMENTO AOS REQUISITOS DE SEGURANÇA, AOS PADRÕES DE BOAS PRÁTICAS E DE GOVERNANÇA E AOS PRINCÍPIOS GERAIS NOS SISTEMAS UTILIZADOS. NÃO CUMPRIMENTO DE DETERMINAÇÃO DA ANPD. CONFIGURAÇÃO DE INFRAÇÕES. SANÇÕES DE ADVERTÊNCIAS. MEDIDAS CORRETIVAS.

1. Apesar da inexistência de norma geral e abstrata sobre o tempo razoável para a comunicação ao titular afetado por incidente de segurança, no caso concreto, a Coordenação-Geral de Fiscalização (CGF) indicou reiteradamente o prazo que seria razoável para realizá-la, de modo individualizado. Ante a ausência de comunicação de maneira individualizada até o momento de elaboração deste Relatório de Instrução, foi caracterizada a violação ao art. 48 da LGPD.

2. Não se sustenta o argumento de equiparação da comunicação geral à comunicação individual do incidente de segurança, independentemente de a comunicação geral eventualmente cumprir com os requisitos previstos no art. 48, §1º, da LGPD.

3. A obrigação de comunicação de incidente à ANPD e aos titulares independe de concretização de danos aos titulares em razão do incidente, bastando que este possa acarretar-lhes risco ou dano relevante. A comunicação oferece aos titulares possibilidade de atuar para se proteger, evitar ou mitigar os potenciais riscos ou danos decorrentes do incidente.

4. A não adoção de sistemas estruturados em conformidade aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais da LGPD configura uma violação ao art. 49, da LGPD. A mera insuficiência de provas que confirmem a falha no sistema como causa do incidente não se sustenta como pretexto para o afastamento de imputação de violação ao artigo em questão.

5. A autuada infringiu os arts. 48 e 49 da LGPD, ensejando a aplicação de 2 (duas) sanções de advertência, cumulada com 3 medidas corretivas.

6. Há adequação da advertência para infrações graves diante da impossibilidade de outra sanção, em atenção ao princípio da proporcionalidade.

3. REFERÊNCIAS

3.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

3.2. Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 01, de 08 de março de 2021.

3.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021 – doravante Regulamento de Fiscalização.

3.4. Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 – doravante Regulamento de Dosimetria.

3.5. Processo de Comunicação de Incidente de Segurança (CIS) nº 00261.001037/2022-06.

3.6. Processo Administrativo Sancionador nº 00261.001963/2022-73.

3.7. Aviso nº 27/2022/CGF/ANPD (0042401).

3.8. Nota Técnica nº 81/2022/CGF/ANPD (0050469).

3.9. Auto de Infração nº 11/2022/CGF/ANPD (0050468).

3.10. Prestação de Informações - Ofício nº 605/2022-GS/SDSCJ (0042409).

3.11. Defesa Administrativa - Ofício nº 780 - GGAJU/SDSCJ (0050475).

3.12. Alegações Finais - Ofício GAB nº 945/2023 – SDSCJPVD (0050490).

3.13. Notas de Esclarecimento (0042414 e 0050478).

3.14. Comunicados publicados no site da Secretaria (0042415; 0042416; 0050476; 0050477).

3.15. Nota Técnica nº 1/2022 GTI (0042413).

4. SUMÁRIO EXECUTIVO DO PROCESSO

4.1. **Auto de Infração:** Auto de Infração nº 11/2022/CGF/ANPD (0050468).

4.2. **Data da lavratura do Auto de Infração:** 07/10/2022

4.3. **Forma da intimação:** (X) Meio eletrônico ( ) Via postal ( ) Pessoal ( ) Comparecimento pessoal ( ) Por edital ( ) Cooperação internacional (X) Outro meio: contato telefônico.

4.4. **Data da intimação:** 07/10/2022 - Certidão SDSCJPVD – Certidão de Intimação Cumprida 3710142 (0050471) e E-mail (0050472).

4.5. **Dispositivos legais e regulamentares infringidos, nos termos do auto de infração:**

a) Lei Geral de Proteção de Dados (LGPD):

Art. 48 – ausência de comunicação ao titular da ocorrência de incidente de segurança que possa acarretar-lhe risco ou dano relevante.

Art. 49 – não utilização de sistema adequado ao tratamento de dados pessoais.

4.6. **Data da apresentação da defesa:** 08/11/2022. Documentos:

i) E-mail Resposta SDSCJ-PE (0050473);

ii) Anexo Resposta SDSCJ-PE (0050474);

iii) Defesa Administrativa (Ofício 780/2022 /GGAJU/SDSCJ, 0050475);

iv) Anexo Comunicado Oficial (0050476);

v) Anexo Comunicado Oficial - Setor SESES (0050477);

vi) Anexo Nota de Esclarecimento (0050478); e

vii) Formulário de CIS (0050479).

4.7. **Produção de prova(s) pelo autuante:** (X)Não ( )Sim. Se sim, informar quais:

4.8. **Produção de prova(s) pela ANPD:** (X) Não ( )Sim.

4.9. **Terceiro(s) interessado(s):** (X) Não ( )Sim.

4.10. **Termo de Ajustamento de Conduta:** (X)Não ( )Sim.

4.11. **Alegações Finais:** ( )Não (X)Sim - Alegações Finais (0050490) e Anexo às Alegações Finais (0050491)

4.12. **Medidas preventivas aplicadas - art. 32 do Regulamento de Fiscalização:** ( )Não (X)Sim - AVISO nº 27/2022/CGF/ANPD (0042401).

4.13. **Medidas preventivas aplicadas - art. 26, IV, do Decreto nº 10.474/2020:** (X)Não ( )Sim.

5. RELATÓRIO

5.1. Conforme disposto no art. 37 do Regulamento de Fiscalização da ANPD, o processo administrativo sancionador destina-se à apuração de infrações à legislação de proteção de dados que sejam de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD. De acordo com o art. 54 do mencionado Regulamento, o Relatório de Instrução subsidiará a decisão de primeira instância, a ser proferida pela Coordenação-Geral de Fiscalização (CGF). Assim, em consonância com os ditames normativos aplicáveis ao caso e demais documentos que constam dos autos, passa-se ao detalhamento dos atos processuais até a presente data, com o objetivo de avaliar os motivos da autuação e os argumentos apresentados pela autuada face à legislação e às normas de proteção de dados.

5.2. Em 17/05/2022, foi instaurado, pela CGF, o Processo de Comunicação de Incidente de Segurança (CIS) nº 00261.001037/2022-06, fruto

de comunicação dessa natureza, apresentada pela então Secretaria de Desenvolvimento Social, Criança e Juventude (SDSCJ)[4], atual Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS)[5], sucessora da Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas (SDSCJPVD) (0042386). A referida CIS informou uma provável falha operacional do sistema ou falha de algum usuário da Secretaria, o que teria propiciado a exposição indevida de dados cadastrais e dados de saúde de 413[6] cadastrados no Programa PE Livre Acesso Intermunicipal, iniciativa que concede gratuidade a pessoas com deficiência em transportes intermunicipais. Os dados teriam sido expostos em uma planilha de dados no site da Secretaria e seria possível "navegar pela planilha sem digitar senha" (0042389), além de ser possível a visualização da cópia de documentos.

5.3. De acordo com o relatado na CIS acima mencionada (0042386), o incidente teria ocorrido no mês de abril de 2022, em data não especificada; a SAS teria tomado ciência do incidente no dia 27/04/2022 às 17h20, por meio de aviso emitido pela Gerência de Comunicação; e sua Ouvidoria teria recebido, no dia 28/04/2022, um e-mail do portal de notícias TecMundo informando sobre o vazamento de dados em questão.

5.4. Tendo em vista que a comunicação completa do incidente à ANPD foi realizada apenas no dia 17/05/2022, o atraso foi justificado pela autuada i) pela adaptação à LGPD e, especialmente, ii) pela ocorrência inédita do fato, com a consequente adoção imediata de medidas para corrigir a falha de segurança, que teria se dado no dia 27/04/2022, pouco após às 19h, oportunidade em que a SAS teria entendido que a rapidez na solução não demandaria a comunicação à ANPD, o que foi revisitado após recomendação da Controladoria do Estado de Pernambuco. Além disso, a comunicação aos titulares também não foi realizada, sob a alegação de que i) o incidente estava sendo apurado; ii) a falha de segurança teria sido corrigida rapidamente (duas horas após o conhecimento da falha); e iii) nenhum usuário dos 413 (quatrocentos e treze) teria comunicado qualquer notícia decorrente de vazamento de dados à Superintendência de Apoio à Pessoa com Deficiência (SEAD).

5.5. A autuada alegou que, a fim de prevenir a ocorrência do incidente de segurança, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, e com uso de senha de identificação. Em relação ao momento posterior ao incidente comunicado, a SAS declarou ter XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. Por fim, suscitou que a medida adotada para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados foi a lavratura de um Boletim de Ocorrência nº 22I0319064793 em 12/05/2022 às 17:03h, na Delegacia de Crimes Cibernéticos (0042386, p. 5) [ACESSO RESTRITO - medidas de segurança implementadas em sistema].

5.6. Segundo a autuada, não teriam sido vislumbradas consequências significativas aos titulares de dados, em razão de i) a falha operacional ter sido corrigida em até duas horas do conhecimento da Superintendência de Apoio à Pessoa com Deficiência (SEAD), área que tratava os dados expostos, e ii) o problema ter aparentado se tratar apenas de falha do sistema (0042386, p. 6).

5.7. Após, em 02/06/2022, foi proferido Despacho (0042390)[7] para determinar que a SAS complementasse a CIS, colacionando ao processo, no prazo de 5 (cinco) dias úteis após o recebimento do Despacho:

> a) a comprovação da comunicação individual do incidente a todos os titulares de dados afetados;
>
> b) o relatório de tratamento de incidente incluindo os seguintes detalhes: registros de acessos dos servidores que armazenavam a base de dados comprometida e a causa-raiz do incidente.

5.8. Em 14/06/2022, a pedido do estado de Pernambuco, foi encaminhado, ao Secretário da SAS, o Ofício nº 164/2022/CGF/ANPD/PR (0042395), para reiterar a determinação do Despacho 0042390 [5.7], e de outras providências de instrução processual, no prazo de 5 (cinco) dias úteis. Destacou-se, ainda, que a comunicação aos titulares deveria ser feita em linguagem clara e simplificada, bem como conter aspectos mínimos, previstos no §1º do Art. 48 da LGPD.

5.9. Em 14/07/2022, ante a ausência de resposta por parte da SAS após o prazo concedido, foi emitido o Aviso nº 27/2022/CGF/ANPD (0042401), oportunidade na qual foram concedidos mais 10 (dez) dias úteis a contar do recebimento do Aviso, a fim de que fossem comprovadas as determinações requeridas no Despacho 0042390 e Ofício 0042395, além de requerer informações dos dados de contato do encarregado, consoante abaixo:

> a) a comprovação da comunicação individual do incidente a todos os titulares de dados afetados;
>
> b) o encaminhamento do relatório de tratamento de incidente incluindo os seguintes detalhes: registros de acessos dos servidores que armazenavam a base de dados comprometida e a causa-raiz do incidente;
>
> c) informe os dados atualizados de seu encarregado de proteção de dados pessoais;
>
> d) ratifique ou retifique, no processo 00261.001037/2022-06, a Comunicação de Incidente de Segurança realizada pela senhora Cibele Flávia Santos Lopes, sob pena de descumprimento do art. 48 da LGPD; e
>
> e) informe onde estão sendo divulgados os dados de contato de seu encarregado pela proteção de dados, em atenção ao § 1º do art. 41 da LGPD.

5.10. Ainda em 14/07/2022, o Aviso (0042401) foi encaminhado à SAS por meio do Ofício nº 189/2022/CGF/ANPD/PR (0042402) e reiterado, em 29/07/2022, por meio de e-mail (0042408).

5.11. Em 01/08/2023, a CGF recebeu o Ofício nº 605/2022-GS/SDSCJ (0042409) da SAS, acompanhado dos seguintes documentos: (i) Portarias (0042410e 0042411); (ii) Nota Técnica nº 1/2022 GTI (0042413); (iii) Formulário de Comunicação do Incidente (0042412), (iv) Nota de Esclarecimento (0042414), e (v) comunicados publicados no site da Secretaria (0042415 e 0042416), em resposta ao Aviso nº 27/2022/CGF/ANPD (0042401).

5.12. Segundo o Ofício nº 605/2022-GS/SDSCJ (0042409), o acesso público de planilha contendo dados pessoais dos beneficiários de programa assistencial teria perdurado entre o período de 26/04/2022, às 13:32h (data/hora do vazamento) à 27/04/2022, às 17:20h (data/hora da detecção do incidente). Além disso, a quantidade de titulares afetados teria sido de 412 titulares, o que também foi alterado no novo CIS anexado (0042412). A autuada realizou comunicado geral do incidente, conforme mostra a Nota de Esclarecimento publicada em seu sítio eletrônico, sem, entretanto, haver

comprovação de comunicação de forma individual a cada titular.

5.13. A Nota Técnica nº 1/2022 GTI (0042413), que mais se aproximaria do relatório de tratamento de incidente requerido pela CGF, não apresentou os detalhes solicitados nas determinações da CGF (ver item [5.7], alínea "b)" e [5.9], alínea "b)"), limitando-se a alguns exemplos de acesso e restringindo-se a lapsos temporais sem explicações para sua delimitação.

5.14. Em 11/08/2022, foi proferido Despacho (0042417) atestando que a prestação de informações e documentos comprovaram o cumprimento das determinações das alíneas "c", "d" e "e" do Aviso nº 27/2022/CGF/ANPD (0042401), estando ausente a comprovação das alíneas "a" e "b". Foi dado novo prazo de 10 (dez) dias para a comprovação de comunicação individual aos titulares e do seu respectivo conteúdo.

5.15. O Despacho (0042417) ainda indicou a insuficiência das informações contidas na Nota Técnica nº 1/2022 GTI (0042413), entre elas, a ausência de indicativos de acessos indevidos por meio da própria aplicação web; a falta de esclarecimento da cronologia do incidente, ou seja, a ausência de informação sobre de que maneira teria sido possível apurar o suposto período de duração do incidente; e a vulnerabilidade explorada e as medidas tomadas pela equipe de segurança, "itens que deveriam compor o relatório de tratamento do incidente" (0042417, item 15).

5.16. Após a ausência de resposta da SAS ao Despacho (0042417) (itens [5.13] e [5.15]), encaminhado por meio do Ofício nº 200/2022/CGF/ANPD/PR (0042418), foi emitida a Nota Técnica nº 81/2022/CGF/ANPD (0042425), reiterando o descumprimento das determinações das alíneas "a" e "b" e a ausência de respostas da SAS. Foi indicada a ausência de medidas adequadas para garantir a confidencialidade dos dados, em razão do controle e monitoramento de acesso não terem restado comprovados, ausências essas que levaram o controlador a não esclarecer "a cronologia do incidente, a vulnerabilidade explorada, as medidas tomadas pela equipe de segurança e a causa-raiz do incidente" (ver item 5.10 da Nota Técnica nº 81/2022/CGF/ANPD (0042425).

5.17. Na referida Nota Técnica 81/2022 (0042425), recomendou-se a instauração de processo administrativo sancionador, com base no art. 37 do Regulamento de Fiscalização c/c artigos 52 e 55-J, IV da LGPD, em razão dos possíveis descumprimentos: ao art. 48 da LGPD, por não ter sido realizada pela SAS, no prazo concedido, a comunicação individual à totalidade dos titulares afetados, nos termos do determinado pela CGF; bem como ao art. 49 do referido diploma legal, cujo teor dispõe sobre o uso de sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, e aos princípios gerais previstos na LGPD.

5.18. Ato contínuo, foi proferido o Despacho Decisório nº 9/2022/CGF/ANPD (0042426), que acolheu a Nota Técnica nº 81/2022/CGF/ANPD (0042425)[8], a fim de instaurar o Processo Administrativo Sancionador nº 00261.001963/2022-73 em desfavor da SAS. Foi, então, lavrado o Auto de Infração nº 11/2022/CGF/ANPD (0050468), em 07/10/2022, com a indicação de infração aos arts. 48 e 49, da LGPD.

5.19. A autuada foi intimada em 24/10/2022, conforme Certidão de Intimação Cumprida 3710142 (0050471).

5.20. Em 08/11/2022, sobreveio a defesa administrativa (Ofício 780/2022 /GGAJU/SDSCJ, 0050475), acompanhada dos seguintes documentos: Anexo Comunicado Oficial (0050476); Anexo Nota de Esclarecimento (0050478) e Formulário de CIS (0050479).

5.21. Na Defesa (0050475), o autuado informa que 413 titulares teriam sido atingidos pelo incidente, enquanto a CIS (0050479) juntada aponta o quantitativo de 412 titulares. Ainda, a SAS reitera que o acesso público dos dados teria ocorrido entre o período de 26/04/2022, às 13:32h à 27/04/2022, às 17:20h, sem que houvesse quaisquer provas de tal alegação.

5.22. Alega que a comunicação individual do incidente aos titulares afetados, que incluem crianças e adolescentes, teria sido materializada pelo sítio eletrônico, através da Nota de Esclarecimento (0050478). A referida Nota foi comprovadamente atualizada, com especificações requeridas pela ANPD, incluindo: i) os tipos de dados violados: tipo de deficiência, nome da mãe, e-mail, cópia de foto, cópia de RG, cópia de CPF, cópia de endereço, laudo médico padrão, cópia RG do responsável, cópia CPF do responsável, data cadastro, data empresa, data envio e foto de cartão "VEM LIVRE ACESSO"; ii) quando e como ocorreu o incidente; iii) a quantidade de usuários; e iv) as medidas tomadas pela Secretaria.

5.23. Em Defesa (0050475), a SAS absteve-se de se defender da indicação de descumprimento do art. 49, da LGPD, constando apenas da CIS (0050479) as medidas de segurança técnicas e administrativas tomadas em relação ao incidente, sem comprovar que seus sistemas estavam estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, e aos princípios gerais previstos na LGPD quando da ocorrência do incidente.

5.24. A autuada não apresentou complementação ao aparente relatório de tratamento de incidente colacionado aos autos previamente (Nota Técnica nº 1/2022 - 0042413) que incluísse os registros de acessos dos servidores que armazenavam a base de dados comprometida e a causa-raiz do incidente.

5.25. Não houve solicitação para produção de novas provas conforme disposto no artigo 48 do Regulamento de Fiscalização.

5.26. Em 18/11/2022, o processo foi sobrestado pelo Despacho (0050480), até que o Regulamento de Dosimetria e Aplicação de Sanções Administrativas fosse aprovado, o que ocorreu em 27/02/2023. Em seguida, em 19/04/2023, a tramitação do presente PAS foi retomada, conforme o Despacho (0050481).

5.27. Em 15/09/2023, a SAS foi intimada pelo Ofício nº 23/2023/FIS/CGF/ANPD (0050482) a apresentar alegações finais no prazo de 10 (dez) dias úteis, a partir da ciência do Ofício (0050482). Em razão do insucesso da intimação, em 26/10/2023, a CGF expediu o Ofício nº 43/2023/FIS/CGF/ANPD (0050484), novamente sem sucesso. Foi, então, expedido o Ofício nº 47/2023/FIS/CGF/ANPD (0050486) em 31/10/2023, cujo recebimento ocorreu em 09/11/2023, conforme Ofício GAB nº 924/2023 – SDSCJPVD (0050488).

5.28. Em 16/11/2023, a SAS apresentou suas Alegações Finais, por meio do Ofício GAB nº 945/2023 – SDSCJPVD (Alegações Finais, 0050490), com o documento Anexo às Alegações Finais (0050491), tempestivamente.

5.29. É o relatório.

6. PRELIMINARES

Competência

6.1. A Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), art.

5º, I, considera dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável". Os dados envolvidos no incidente de segurança aqui tratado – tipo de deficiência, nome da mãe, e-mail, cópia de foto, cópia de RG, cópia de CPF, cópia de endereço, laudo médico padrão, cópia RG do responsável, cópia CPF do responsável e foto de cartão "VEM LIVRE ACESSO" – são dados pessoais (alguns até mesmo sensíveis), pois consistem em informação relacionada a pessoa natural identificada ou identificável.

6.2. A leitura do processo revelou que a atividade desenvolvida pela SAS configura tratamento de dados pessoais, já que realizava, ao menos, a coleta, o armazenamento e a análise desses dados para conceder os cadastros dos titulares no Programa PE Livre Acesso, de modo que as operações se enquadram na previsão do art. 5º, X, que classifica como tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"

6.3. A LGPD, ainda, define a figura do controlador no art. 5º, VI, como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Tendo em vista que a SAS efetuou o tratamento de dados pessoais para operacionalizar uma política pública de transporte, resta estabelecido que a ela competem as decisões referentes ao tratamento de dados pessoais, motivo pelo qual é controladora.

6.4. A circunstância de a atividade realizada pela SAS na gestão do Programa PE Livre Acesso estar inserida nas disposições da LGPD implica a competência de atuação da ANPD, definida pelo art. 5º, XIX da mencionada Lei, como "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional". Cabe à ANPD, de acordo com o art. 55-J, "I - zelar pela proteção dos dados pessoais, nos termos da legislação", bem como "IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso" e "XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos".

6.5. No âmbito da ANPD, a Coordenação-Geral de Fiscalização (CGF) é a responsável por identificar as infrações à LGPD. De acordo com o Regimento Interno da ANPD:

> Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:
>
> I - fiscalizar e aplicar as sanções previstas no artigo 52 da Lei nº 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> [...]
>
> III - promover ações de fiscalização sobre as ações de tratamento de dados pessoais efetuadas pelos agentes de tratamento, incluído o Poder Público;
>
> [...]
>
> VII - receber as notificações de ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares e dar o tratamento necessário;
>
> [...]
>
> IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

6.6. O art. 48 do Regimento Interno da ANPD determina, ademais, que as "atividades da ANPD obedecerão, além dos princípios estabelecidos na Lei nº 13.709, de 2018, aos princípios da legalidade, motivação, moralidade, eficiência, celeridade, interesse público, impessoalidade, igualdade, devido processo legal, ampla defesa, contraditório, razoabilidade, proporcionalidade, imparcialidade, publicidade, economicidade, segurança jurídica, entre outros". Esta é, portanto, a justificativa para análise da atividade desenvolvida pela SAS em processo administrativo próprio, pois é necessário observar as diretrizes e os princípios incidentes sobre a atuação administrativa no cumprimento da atribuição de fiscalização.

6.7. O Regulamento de Fiscalização da ANPD dispõe sobre a estruturação das atividades previstas no art. 17 do Regimento Interno da ANPD. De acordo com o art. 2º do Regulamento, a fiscalização volta-se ao monitoramento, à orientação, à prevenção e à repressão das infrações à LGPD, de sorte a, conforme o art. 3º, proteger os direitos dos titulares de dados, promover a implementação da legislação de proteção de dados pessoais e zelar pelo cumprimento das disposições da LGPD.

6.8. Diante das referidas competências, em especial da atividade preventiva, a Autoridade constatou, na hipótese presente, que haveria risco ou dano relevante aos titulares devido à gravidade do incidente de segurança em questão, em razão dos tipos de dados afetados, bem como a vulnerabilidade dos titulares (0042390), de modo que a SAS deveria comunicar sua ocorrência aos titulares, sob pena de descumprimento do art. 48 da LGPD. De tal ocorrido, resultou a análise individualizada do caso, fato que deu início ao Processo de CIS nº 00261.001037/2022-06, que culminou no presente Processo Administrativo Sancionador nº 00261.001963/2022-73.

6.9. Ademais, por força do art. 4º, I, do mencionado Regulamento, a SAS é considerada agente regulado pela ANPD, haja vista ser um agente de tratamento – no caso, controladora (item [6.3]). Cumpre especificar os deveres a que os agentes regulados estão submetidos:

> Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros:
>
> I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;
>
> II - permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;
>
> III - possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados

e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;

IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;

V - manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e

VI - disponibilizar, sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.

6.10. Pelo exposto, fica estabelecida a competência da ANPD no caso concreto para avaliar a conduta da SAS, controladora de dados e agente regulado, à luz da LGPD.

Outras questões preliminares

6.11. A autuada não arguiu questões preliminares de mérito em sua defesa, tampouco esta CGF verificou a existência de tais questões a serem trazidas a este Relatório de Instrução.

7. ANÁLISE

Circunstâncias da infração e autoria

7.1. Os documentos apresentados aos autos são suficientes para afirmar que houve um incidente de segurança no sistema da autuada, utilizado para o gerenciamento de cadastro de usuários no Programa PE Livre Acesso, o qual resultou na disponibilização de dados pessoais e pessoais sensíveis de titulares (tipo de deficiência, nome da mãe, e-mail, cópia de foto, cópia de RG, cópia de CPF, cópia de endereço, laudo médico padrão, cópia RG do responsável, cópia CPF do responsável e foto de cartão "VEM LIVRE ACESSO") [5.22], incluindo de crianças e adolescentes, consoante informado pela própria Secretaria, por CIS (0042386), reiterado na CIS atualizada (0042412).

7.2. A exposição indevida de dados pessoais, incluindo diversos dados cadastrais e de saúde de pessoas cadastradas no programa, nome da mãe do titular e de eventuais responsáveis, configura a ocorrência de um incidente de segurança capaz de acarretar risco ou dano relevante aos titulares dos referidos dados. Ademais, o incidente foi confirmado pela autuada na Defesa Administrativa (0050475) e nas Alegações Finais - Ofício GAB nº 945/2023 – SDSCJPVD (0050490).

7.3. Durante todo o Processo de Fiscalização anterior a este PAS (Processo de CIS nº 00261.001037/2022-06), a CGF determinou à SAS a adoção de medidas relacionadas ao incidente, no que não foi atendida. As determinações em questão relacionam-se à: i) comunicação do incidente aos titulares de dados, a qual não foi realizada de maneira individualizada, tão somente de forma coletiva (ver itens [5.11] a [5.22]); e ii) ausência de demonstração da causa do incidente e a respectiva adoção ou não de requisitos de segurança que estivessem presentes nos sistemas utilizados para o tratamento de dados pessoais (ver itens [5.7], [5.8] e [5.9]), que poderiam ter sido comprovados, por exemplo, por meio da elaboração do relatório de tratamento de incidente de segurança, apresentado de forma parcial à Autoridade (ver itens [5.12] e [5.24]).

7.4. Além disso, tendo em vista que a variação da quantidade de titulares que foram impactados no incidente, oscilando entre 412 e 413 titulares, conforme alegações da SAS (ver nota de rodapé nº 6), esta CGF considerará que o número de afetados foi de 413 (quatrocentos e treze) titulares, adotando a abordagem mais protetiva aos titulares, a fim de que nenhum titular possa ser prejudicado quando da execução de medidas corretivas a serem adotadas pela SAS, conforme determinações do item [8.1].

7.5. **Restam comprovados, assim, os fatos que ensejaram a instauração deste PAS e a autoria por parte da autuada.**

Conduta: não comunicar aos titulares a ocorrência de incidente de segurança que possa lhes acarretar risco ou dano relevante – art. 48 da LGPD.

Defesa apresentada pela autuada

7.6. **A comunicação do incidente de forma individualizada aos titulares de dados não foi realizada ou ao menos comprovada.** Em sua primeira manifestação, no Formulário CIS (0042386), a SAS alegou que a ausência de comunicação do incidente aos titulares de dados teria decorrido de três fatores: i) o incidente estava sendo apurado; ii) a falha de segurança teria sido corrigida rapidamente (duas horas após o conhecimento da falha); e iii) nenhum usuário dos 413 (quatrocentos e treze) teria comunicado qualquer notícia decorrente de vazamento de dados à Superintendência de Apoio à Pessoa com Deficiência (SEAD).

7.7. A autuada relatou e reprisou, em todas as suas manifestações subsequentes ao Formulário CIS (0042386), que teria realizado a comunicação **individual** aos titulares do incidente de segurança no site próprio da SAS, de tal sorte que a **autuada considerou a comunicação destinada ao público em geral como uma comunicação individualizada a cada titular de dados** (vide: Prestação de Informações - Ofício nº 605/2022-GS/SDSCJ [0042409] e documentos anexos: Nota de Esclarecimento [0042414] e captura da tela dos comunicados publicados no site da Secretaria [0042415e 0042416]; Defesa Administrativa - Ofício nº 780 - GGAJU/SDSCJ [0050475] e documentos anexos: Anexo Comunicado Oficial [0050476], Anexo Comunicado Oficial - Setor SESES [0050477] e Anexo Nota de Esclarecimento [0050478]; e Alegações Finais - Ofício GAB nº 945/2023 – SDSCJPVD [0050490] e Anexos Anexo às Alegações Finais [0050491]).

7.8. Em sua Defesa Administrativa (0050475), a SAS reprisa sua argumentação no fato de que a comunicação individual do incidente teria sido comprovada com os comunicados oficiais divulgados no site, juntando nova Nota de Esclarecimento (0050478) e print da nova página em que tal Comunicado Oficial teria sido disponibilizado (0050477).

7.9. Em Alegações Finais (0050490), a autuada limita-se a reforçar os argumentos suscitados na Defesa Administrativa (0050475), sem justificar a ausência de comunicação individualizada aos titulares de dados afetados no incidente de segurança.

Subsunção do fato ao tipo infracional correspondente

7.10. O art. 48 da LGPD determina que cabe ao controlador comunicar

à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Nos termos do §1º do mencionado artigo, a comunicação deverá ser feita em prazo razoável, a ser regulamentado pela ANPD. Ainda que pendente a regulamentação do prazo para a comunicação do incidente, o §2º do art. 48 da LGPD confere à ANPD o poder de determinar ao controlador providências para a salvaguarda dos direitos dos titulares, tais como medidas para reverter ou mitigar os efeitos do incidente e a ampla divulgação do fato em meios de comunicação.

7.11. Ocorre que, no caso em comento, a infratora realizou apenas a comunicação geral, não individualizada, mesmo após reiteradas requisições da ANPD. Conforme relatado, a autuada informou a ocorrência do incidente à ANPD em 17/05/2022, tendo a CGF indicado reiteradamente a necessidade de a SAS realizar a comunicação do incidente de forma individual aos titulares (Despacho [0042390], em 02/06/2022, determinou a comunicação em até 5 (cinco) dias úteis; Ofício [0042395], em 14/06/2022, determinou a comunicação em até 5 (cinco) dias úteis; e Aviso [0042401], em 14/07/2022, em sede de medida preventiva, determinou a comunicação em até 10 (dez) dias úteis).

7.12. Em 25/07/2022, em atenção ao Aviso (0042401), a autuada prestou informações (0042409) sobre o fato de que a comunicação do incidente por meio da Nota de Esclarecimento publicada no site da SAS seria equivalente à obrigação da comunicação individual dos titulares.

7.13. Em seguida, **a CGF reprisou que a comunicação aos titulares deveria ser realizada de forma individualizada** (Despacho [0042417], em 11/08/2022, determinou a comunicação em até 10 (dez) dias úteis), **de modo que a alegação da autuada de que a comunicação no site se equipararia à comunicação individual não se sustentava e tampouco atingia requisitos mínimos do art. 48, §1º, da LGPD.**

7.14. Isso, porque i) o quantitativo de titulares seria definido e limitado (412 titulares), de forma que a medida não seria desarrazoada ou desproporcional; ii) a autuada possuía cópia de endereços e e-mails, sendo factível que o contato pudesse ser efetuado, seja de forma física ou virtual; e iii) o comunicado geral a) foi divulgado em página web diferente da página de cadastro para a utilização do serviço público em questão (programa PE Livre Acesso), o que diminuiria a probabilidade de um titular acessá-lo e b) não incluía em seu conteúdo as informações mínima elencadas pelo art. 48, §1º, da LGPD. Por fim, a Nota Técnica nº 81/2022/CGF/ANPD (0042425) emitida em 08/09/2022, reiterou os argumentos acima elencados, além de recomendar a instauração do PAS em comento.

7.15. Mesmo diante de tais argumentos, a SAS deliberadamente optou por não realizar a comunicação individual, mas tão somente atualizar a Nota de Esclarecimento disponibilizada em seu sítio eletrônico, consoante colacionado aos autos (0050478 e 0050477)[9], nos termos apontados pelo Despacho (0042417) e reiterados pela Nota Técnica nº 81/2022/CGF/ANPD (0042425) (itens [7.13] e [7.14]).

7.16. Portanto, a inércia da autuada frente à determinação de CIS individual se prolonga por um período extenso e injustificado, especialmente em razão de: i) o quantitativo de titulares ser praticamente definido e limitado (entre 412 e 413 titulares), de forma que a medida não seria desarrazoada ou desproporcional, o que permitiria o envio de mensagens, ainda que manualmente, caso não houvesse disponibilidade de soluções que tornassem mais ágil essa atividade; ii) a CGF já ter apontado que a comunicação individual poderia ser materializada por meio físico ou eletrônico; e iii) a autuada sempre ter tido em seu poder a informação sobre os titulares afetados, seus e-mails de contato e seus endereço físicos, consoante aclaramentos concedidos pela SAS e pela consulta realizada por esta CGF ao formulário de cadastro no programa PE Livro Acesso disponibilizado no sítio eletrônico da Secretaria[10].

7.17. Ainda, em que pese a Nota de Esclarecimento tenha sido publicada em nova página do sítio web da SAS (https://www.sdscjpvd.pe.gov.br/seses/pe-livre-acesso-intermunicipal/), alinhada ao apontado pela ANPD (0042417), a Nota persiste na página web anterior em versão desatualizada (https://www.sdscjpvd.pe.gov.br/lgpd/).

7.18. Por todo o exposto, considerando que a autuada foi silente quanto ao não cumprimento da determinação de comunicação individual, fazendo crer que a comunicação generalizada supriria a necessidade de comunicação individualizada apesar de reiteradas manifestações da CGF em contrário e tendo em vista o período transcorrido entre o conhecimento do incidente até a atualidade, **configura-se a violação ao art. 48 da LGPD.**

Classificação da infração

7.19. O art. 48, caput e incisos, determina que o controlador deve apresentar CIS adequada tanto à ANPD quanto ao titular em prazo razoável. Conforme visto nos itens [7.10] a [7.17], a autuada não fez comunicado individual com conteúdo adequado aos titulares afetados pelo incidente de segurança.

7.20. Segundo prevê o Regulamento de Dosimetria, a infração pode ser considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares. Nesse sentido, a falta de CIS ao titular em prazo razoável pode ser classificada como média sob quatro aspectos, nos termos do art. 8º, §2º, do Regulamento de Dosimetria.

7.21. Em primeiro lugar, o incidente ocorrido i) resultou na exposição de dados pessoais envolvendo dados de saúde e dados de crianças e adolescentes; e ii) permitiu que terceiros pudessem acessar um volume considerável de dados relativos a cada um dos usuários individualmente, ainda que o volume de titulares afetados como um todo não tenha sido tão expressivo.

7.22. Em segundo lugar, a eventual atividade de tratamento decorrente do incidente pode impedir ou limitar que os usuários tenham garantido seu direito de acesso ao programa de concessão de gratuidade em transportes intermunicipais, caso seus dados sejam, por exemplo, duplicados e utilizados por terceiros para o uso do mesmo serviço, impedindo o uso pelo verdadeiro titular, o que limitaria o exercício do direito de livre locomoção, capaz de causar danos materiais aos titulares.

7.23. Em terceiro lugar, intimamente atrelado aos parâmetros anteriores, os dados expostos no caso concreto (tipo de deficiência, nome da mãe, e-mail, cópia de foto, cópia de RG, cópia de CPF, cópia de endereço, laudo médico padrão, cópia RG do responsável, cópia CPF do responsável e foto de cartão "VEM LIVRE ACESSO") permitem que o titular possa sofrer danos em situações, por exemplo, de discriminação, violação à imagem, perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos. Isso é especialmente relevante ao ponderar-se que a conjugação de múltiplos dados relativos a uma mesma pessoa pode facilitar que mais ações de fraudes possam ser efetuadas em seu nome, além de conferir maior plausibilidade de que o terceiro seja reconhecido como o verdadeiro titular dos dados expostos.

7.24. Por fim, em quarto lugar, a conclusão a que se chega dos elementos supracitados é a de que a falta de conhecimento sobre o incidente impede que o titular possa i) exercer o seu direito fundamental à proteção de dados e ii) diminuir possíveis consequências causadas à inviolabilidade da privacidade, da honra e da imagem, já que diversas são as hipóteses de danos, como acima relatado, caso não sejam tomadas as precauções necessárias por parte do titular.

7.25. Congruente a isso, o Cert.br/Nic.br/Cgi.br, com contribuição da ANPD, elaborou o Fascículo de "Vazamento de Dados"[11], cujo objetivo é informar algumas medidas que podem ser tomadas pelos titulares para a redução do impacto de eventuais vazamentos de dados. A relevância de a CIS ser realizada para o titular, portanto, decorre do fato de que o titular, após ter conhecimento sobre um incidente de segurança que o tenha afetado, pode adotar algumas providências, como as já divulgadas no documento.

7.26. A comunicação do incidente de segurança por meio de informação pública no site não assegura que todos os usuários afetados venham a tomar conhecimento do ocorrido. Por isso a necessidade de comunicação individual, direta e personalizada, conforme determinado e reiterado pela CGF. A ausência de CIS individual prejudica o alcance da comunicação, e resulta na ausência de adoção de cuidado qualificado por parte de tais titulares; na diminuição da probabilidade de um titular exigir mais segurança da controladora de dados ora autuada; e na maior dificuldade de o titular de exercer seus direitos perante tal, que deve agir de modo a evitar o uso indevido de tamanho volume de dados, em especial pelo envolvimento de dados de saúde e de crianças e adolescentes.

7.27. Logo, a infração ao art. 48 ora analisada se enquadra nos requisitos do art. 8º, §2º, do Regulamento de Dosimetria, atendendo ao critério para ser classificada como média.

7.28. Além disso, no presente caso, a infração de falta de CIS versa sobre dados sensíveis (tipo de deficiência e laudo médico) e dados de crianças e adolescentes (consoante relatado no Formulário de CIS [0042386]). Essas características elevam o grau de classificação da infração que, por esse motivo, **passa a ser considerada como grave, segundo art. 8º, §3º, "d", do Regulamento de Dosimetria**[12].

Definição do tipo de sanção administrativa

7.29. Para a definição do tipo de sanção adequada, o art. 9º do Regulamento de Dosimetria indica ser aplicável multa simples quando a infração for classificada como grave. No entanto, o art. 52, §3º da LGPD, ao estabelecer as sanções que podem ser impostas a entidade ou a órgãos públicos, afasta, por omissão, a possibilidade aplicação de multa ou de multa diária a esses agentes de tratamento. Por outro lado, o Regulamento de Dosimetria define, em seu art. 9º, que a advertência somente pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medida corretiva.

7.30. Considerando que a infração foi classificada como grave, seria afastada, em princípio, a possibilidade de aplicação da sanção de advertência com fundamento no art. 9º, I, do Regulamento de Dosimetria. Todavia, o art. 9º, II, do Regulamento de Dosimetria indica que a sanção de advertência é igualmente adequada quando houver necessidade de imposição de medidas corretivas. Esta hipótese se aplica à presente infração, tendo em vista a necessidade de impor à autuada a realização de comunicação, desta vez individualizada, em atenção ao disposto no §1º do art. 48, da LGPD.

7.31. Diante do exposto, tendo em vista que persiste a necessidade de comunicação individualizada aos titulares afetados pelo incidente de segurança, impõe-se as seguintes medidas corretivas, acompanhadas de suas comprovações:

a) envio de comunicação direta e individualizada a cada um dos 413 titulares afetados pela exposição dos dados no sítio eletrônico da SAS. A proporcionalidade desta medida decorre do fato de que a SAS sujeita o próprio cadastro dos titulares no programa à submissão de seus respectivos e-mails e endereços físicos.

i. O teor da comunicação individual poderá ser o mesmo da segunda versão da Nota de Esclarecimento (0050478), desde que: i) sejam incluídos os motivos da demora da comunicação, por não ter sido imediata, consoante art. 48, §1º, V, da LGPD; ii) sejam alteradas as informações eventualmente desatualizadas, como, por exemplo, os dados do encarregado e o que mais a SAS entender necessário.

ii. A fim de se comprovar o cumprimento da medida corretiva, determina-se à SAS que junte aos autos, **no prazo de 20 (vinte) dias úteis** contados nos termos do art. 12, I, do Regulamento de Fiscalização, comprovação de que a medida corretiva "a)" descrita no item [7.31] foi cumprida por meio da apresentação de uma planilha com a lista completa de todos os 413 titulares afetados identificados que foram individualmente comunicados contendo (i) o nome completo do titular; (ii) data de contato; (iii) informação de contato utilizada para a comunicação individual (o número de telefone, se por meio telefônico; o e-mail, se por correio eletrônico; o endereço, se por meio físico etc); e iv) o envio do inteiro teor de 40 comunicações realizadas por e-mail ou por meio físico, a fim de que seja possível que a CGF valide, por amostragem, a comunicação feita ao titular.

b) atualização da CIS geral no sítio eletrônico da SAS, conforme segunda versão juntada aos autos (0050478), incluídas as alterações mencionadas no item [7.31], alínea "a)", primeira subalínea "i", na página em que os usuários se cadastram no Programa PE Livre Acesso (https://www.sdscjpvd.pe.gov.br/seses/pe-livre-acesso-intermunicipal/ ou correspondente), bem como na página específica relacionada à LGPD (https://www.sas.pe.gov.br/lgpd/ ou correspondente), e sua manutenção, por pelo menos mais 90 (noventa) dias corridos a contar da data da intimação da decisão deste PAS. Essa medida é importante para que os titulares tenham mais um veículo de comunicação para tomar ciência do incidente em questão e buscar mais informações junto à SAS.

i. Deverá ser juntada aos autos comprovação de que a medida corretiva do item [7.31] "b)" foi cumprida por meio da apresentação de, pelo menos, 9 (nove)

capturas de tela de cada um dos sítios eletrônicos acima indicados da SAS contendo o comunicado e com visualização clara da data da captura, sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma.

ii. A comprovação de cumprimento da medida corretiva deverá ser juntada aos autos em até 5 (cinco) dias úteis do final de cada período de 30 (trinta) dias, independentemente de nova intimação para tanto.

7.32. Embora tenha sua análise mitigada no presente processo (uma vez que não será aplicada a sanção de multa), registra-se a existência de circunstância agravante existente no caso concreto, tendo em vista que a autuada deixou de cumprir a determinação apresentada no Aviso nº 27/2022/CGF/ANPD (0042401) [7.12], medida preventiva adotada no âmbito do Processo de CIS, nos termos do art. 32, II, do Regulamento de Fiscalização. Identificada, portanto, a ocorrência de uma circunstância agravante, nos termos do art. 32, §2º, II, do Regulamento de Fiscalização e do art. 12, III, do Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

7.33. **Fica, portanto, cominada a sanção de advertência cumulada com medidas corretivas para a infração ao art. 48 da LGPD**.

Conduta: não utilizar sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios da LGPD – art. 49 da LGPD (incidente de segurança).

Defesa apresentada pela autuada

7.34. Como consta dos autos, foi relatado pela autuada a ocorrência de um incidente de segurança com dados pessoais em razão de uma “falha operacional do sistema ou de algum usuário da secretaria” (0042386, p. 3). Resultou do referido incidente a exposição de dados pessoais e dados pessoais sensíveis que estavam sob a guarda da SAS, em virtude de cadastro de pessoas com deficiência no programa PE Livre Acesso Intermunicipal, cujo objetivo é a concessão de gratuidade a tal grupo de pessoas em transportes intermunicipais.

7.35. Além disso, nos termos informados pela SAS, a “falha operacional foi corrigida em até duas horas do conhecimento da SEAD” (0042386, p. 6), de forma que não teriam sido vislumbradas “consequências significativas para os titulares de dados, pois aparenta que o problema se tratou apenas de falha do sistema” (0042386, p. 6).

7.36. De acordo com o Formulário de CIS (0042386), a autuada afirmou que realizaria relatório de impacto à proteção de dados pessoais até 30/07/2022 (prazo prorrogado na Nota de Esclarecimento [0050478] para 30/08/2022). Entretanto, não houve a apresentação do referido documento de RIPD no âmbito deste PAS.

7.37. Ainda no Formulário de CIS (0042386), a autuada relatou as seguintes medidas de segurança técnicas e administrativas que teriam sido adotadas:

i) para prevenir a ocorrência do incidente de segurança: a “XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX” (0042386, p. 5) [ACESSO RESTRITO - medidas de segurança implementadas em sistema];

ii) após a ciência do incidente de segurança: “XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX” (0042386, p. 5) [ACESSO RESTRITO - medidas de segurança implementadas em sistema];

iii) para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados, tais medidas foram limitadas à lavratura do “Boletim de Ocorrência nº 22I0319064793 em 12/05/2022, às 17:03h na Delegacia de Crimes Cibernéticos” (0042386, p. 5).

7.38. No referido Boletim de Ocorrência, registrou-se que a planilha com dados pessoais que era “protegida por senha passou a poder ser acessada para leitura, indevidamente e sem autorização dos gestores, por meio da internet" (0042386, p. 9).

7.39. Na prestação de informações e documentos (0042409) apresentada pela SAS, em resposta ao Aviso (0042401), a autuada informou que o acesso público dos dados pessoais dos beneficiários de programa assistencial teria remanescido entre o período de 26/04/2022, às 13:32h (data/hora do vazamento), a 27/04/2022, às 17:20h (data/hora da detectação do incidente). Para mais, relatou, genericamente, que as medidas de segurança técnicas e administrativas necessárias, incluindo a comunicação da ocorrência à ANPD, teriam sido adotadas. Ademais, foi colacionada aos autos a primeira versão da Nota de Esclarecimento publicada no site da autuada (0042414).

7.40. Junto à prestação de informações, foi apresentada a Nota Técnica nº 1/2022, elaborada pela Gerência de Tecnologia da Informação (0042413) em 25/07/2022, em que foi informada a inexistência de evidências de acessos indevidos aos servidores de aplicação e de bancos de dados no período entre 25 e 28 de abril de 2022. Para fins exemplificativos, foram apresentados alguns acessos aos servidores de aplicação e de bancos de dados, constando pontos de acesso relativos aos meses de março, abril e junho de 2022. Ademais, a Nota Técnica nº 1/2022 GTI da SAS (0042413) relata que não havia histórico superior a 30 dias sobre tentativas sem sucesso nos servidores.

7.41. Em sede de Defesa Administrativa (0050475), foi reiterada a informação de que o incidente teria decorrido de falha operacional do sistema ou de algum usuário da Secretaria, sem a confirmação da causa-raiz do incidente.

7.42. Destaca-se que, na Defesa (0050475), os argumentos suscitados em suas manifestações anteriores foram repisados, com a adição dos esclarecimentos da Nota de Esclarecimento – LGPD, em que foi mencionada a adoção de medidas adicionais: “d) Estabelecimento de prazo interno para capacitação da equipe da Secretaria Executiva de Segmentos Sociais (Seses) sobre a importância da implantação do LGPD no tratamento de dados pessoais dos beneficiários dos programas de assistência social sob sua responsabilidade, conforme cronograma de cursos oferecidos pelo Centro de Formação dos Servidores e Empregados Públicos do Estado de Pernambuco (Cefospe); e) Estabelecimento de prazo interno para início da campanha de conscientização quanto ao uso responsável da informação e tratamento de dados, até 31/12/2022; (...) g) Confecção de Relatório Interno de Impacto a Proteção de Dados Pessoais, até 30/08/2022, para avaliação, dentre outros, da natureza, categoria e quantidade de titulares afetados e das consequências concretas e prováveis.” (0050478, p. 26).

7.43. Em Alegações Finais (0050490), a SAS reiterou as razões supracitadas, além de relatar que foram desenvolvidos procedimentos de

comunicação ao Controlador e à Controladoria do Estado para suporte dos procedimentos. Não acrescentou, porém, nenhuma informação nova sobre a adequação do sistema utilizado para o tratamento de dados realizado.

Subsunção do fato ao tipo infracional correspondente

7.44. Viola o art. 49 da LGPD o sistema utilizado para tratar dados pessoais que não seja estruturado de modo a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na lei e às demais normas regulamentares.

7.45. Em princípio, cumpre esclarecer que a constatação de todo o incidente de segurança parte do pressuposto da existência de um evento adverso confirmado, relacionado à violação de determinadas propriedades da segurança de dados pessoais[13]. Ao receber a comunicação de incidente de segurança (CIS), a ANPD atuará junto com o agente de tratamento para assegurar os direitos dos titulares de dados e averiguar se tal incidente representou infrações à LGPD. Por exemplo, é possível que o incidente tenha decorrido de sistemas que não atendam a requisitos de segurança para o tratamento de dados ou que, mesmo com a adoção de medidas de segurança, o incidente não poderia ter sido evitado. É no âmbito do processo de CIS, portanto, que se verificam os motivos que levaram à ocorrência do incidente e as medidas adotadas pelo agente de tratamento – destacando-se que, ainda que se verifiquem irregularidades em face da LGPD, a ANPD irá privilegiar, sempre que possível, a fiscalização responsiva, que prioriza a adoção de medidas para reconduzir o agente de tratamento à conformidade com a Lei e para remediar situações que acarretem risco aos titulares[14].

7.46. No caso em análise, a autuada informou que adotava as seguintes medidas de segurança como medidas preventivas à ocorrência do incidente: “XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (0042386) [5.5]. **Ocorre que as medidas indicadas não foram observadas, pois a planilha pôde ser acessada irrestritamente, no próprio site da Secretaria e sem que houvesse uso de quaisquer tipos de controle de acesso** (0042386; 0042387; 0042389) [ACESSO RESTRITO - medidas de segurança implementadas em sistema].

7.47. Tendo em vista a constatação pela autuada da ausência das medidas de segurança, a CGF considerou ser necessário compreender as razões de tal vulnerabilidade e a causa do incidente de segurança. Por isso, desde o início do Processo de CIS, a CGF solicitou a apresentação de relatório de tratamento do incidente de segurança, que incluísse “registros de acessos dos servidores que armazenavam a base de dados comprometida e a causa-raiz do incidente” (0042390) (ver itens [5.7] a [5.15]).

7.48. Tais informações, no entanto, não foram apresentadas de forma completa nem por meio de um relatório de tratamento de incidente de segurança, nem por outro tipo de documento. Assim, apesar de reiteradamente diligenciada a aportar elementos aos autos do processo de CIS ou aos autos deste sancionador, a autuada falhou em confirmar duas importantes questões para a compreensão do incidente ocorrido:

> i) Em primeiro lugar, não foi confirmado o **início do incidente de segurança**. A autuada afirma que ele teria ocorrido de 26/04/2022, às 13:32h (data/hora do vazamento) à 27/04/2022, às 17:20h (ver item [5.11]); no entanto, não houve a comprovação de data especificada. Essa afirmação foi questionada pela CGF no Despacho 0042417, o qual atestou que não foi possível apurar tal período, em razão da falta de informação apresentada pela autuada (ver item [5.15]); e na Nota Técnica nº 81/2022/CGF/ANPD (0042425), que indica não ter a SAS esclarecido, entre outros elementos, a cronologia do incidente (ver item [5.16]). A autuada, no entanto, não explicou como chegou a essa afirmação, especialmente após a Nota Técnica nº 1/2022 GTI, mencionada no item [5.13], não ter identificado acessos indevidos ou outros elementos que pudessem sugerir o horário que se alega ter ocorrido o incidente em análise.
>
> ii) Em segundo lugar, a autuada falhou em identificar **qual vulnerabilidade do sistema foi explorada ou a causa-raiz do incidente**. Isso, pois a Nota Técnica nº 1/2022 GTI, elaborada pela Gerência de Tecnologia da Informação da SAS (0042413), que mais se enquadraria ao documento exigido, restringiu-se à exposição de exemplos de acessos aos servidores de aplicação e de bancos de dados, sem detalhamento. Ademais, **a análise foi limitada a possíveis acessos indevidos somente em relação ao período entre 25 e 28 de abril de 2022**, descartando a eventualidade de o acesso indevido e a exposição dos dados ter ocorrido antes deste período. Recorde-se, conforme mencionado acima, que o incidente supostamente teria ocorrido entre os dias 26 e 27 de abril de 2022. Constata-se, portanto, a incongruência em delimitar, sem justificativa para tanto, a verificação de acessos a este período de 3 dias, entre os quais foi incluído o dia 28, data em que a autuada já sabia do incidente – o qual, portanto, já havia ocorrido, tornando inócua a averiguação de eventuais acessos indevidos na investigação do incidente em questão. Nesse sentido, o Despacho (0042417) indicou que não restou esclarecida a vulnerabilidade explorada, a forma a que se chegou à conclusão do período de exposição dos dados, tampouco a causa-raiz do incidente (ver item [5.15]).

7.49. Ao longo do processo de CIS que antecedeu este sancionador, a ANPD solicitou à autuada que esclarecesse os dois itens acima elencados (ver itens [5.15] e [5.16]). Na medida em que a autuada não apresentou as informações requeridas, o Auto de Infração (0050468), que inaugura este sancionador, explicitou o entendimento de que o incidente havia decorrido de falhas relacionadas à segurança do sistema utilizado para o tratamento de dados pessoais, ao apontar a suposta infração ao art. 49 da LGPD (ver item [5.18]), de acordo com a motivação apresentada na Nota Técnica nº 81/2022/CGF/ANPD (0050469) (ver item [5.16]).

7.50. A autuada, no entanto, **não apresentou informações, elementos, argumentos ou provas que afastassem tal entendimento**. Isso poderia ter sido feito, por exemplo, pela confirmação de que o sistema utilizado possui requisitos de segurança adequados; pela indicação de que o incidente decorreu de outras circunstâncias – como a falha na adoção de medidas administrativas – que não falha de segurança no sistema; ou, ainda, pela demonstração de que o incidente ocorreu apesar de atuação diligente quanto aos requisitos de segurança do sistema e às medidas de segurança adotadas.

7.51. Diante das provas colacionadas aos autos, não foi demonstrado monitoramento de acesso adequado que fosse capaz de justificar o período

em que a autuada afirma que os dados teriam ficado expostos a acesso público, mediante, exemplificativamente, provas relacionadas a: um acesso indevido nos servidores de aplicação, nas bases de dados ou nas aplicações web; e/ou uma falha humana; e/ou qualquer outra vulnerabilidade, de forma a demonstrar a existência de adequado monitoramento de acesso aos sistemas da autuada.

7.52. Assim, em razão da ausência de informações apresentadas pela autuada à CGF nos dois processos de que foi parte (o de comunicado de incidente de segurança e o presente sancionador), **resta estabelecido que o incidente decorreu da falha de medidas de segurança, a qual comprometeu a confidencialidade da segurança dos dados pessoais descritos no item** [7.1].

7.53. Cumpre destacar que, conforme disposto no Regulamento de Fiscalização, a atuação da Autoridade observa premissas responsivas, mediante as quais se enfatiza a busca pela cooperação do regulado com o regulador e vice-versa, de modo a se reconduzir o agente de tratamento à plena conformidade ou a evitar ou remediar situações que possam acarretar risco ou dano aos titulares de dados pessoais e a outros agentes de tratamento. O objetivo maior da LGPD e, por conseguinte, da ANPD, é que os dados pessoais sejam tratados de acordo com os parâmetros legais; e o diálogo, a interação e a construção dialética com os regulados, por seu caráter educativo e colaborativo, estão entre as maneiras mais efetivas de assegurar que essa finalidade seja alcançada.

7.54. Para tanto, a LGPD conferiu competência legal à ANPD para solicitar e receber informação dos agentes de tratamento, de modo a assegurar o diálogo entre as partes e amplificar as possibilidades de a Autoridade orientar o regulado, reconduzi-lo à conformidade e atuar de maneira preventiva e educativa. O acesso da ANPD às informações dos regulados é tão amplo, que a Lei previu entre as competências do órgão a necessidade de zelar pela observância dos segredos comercial e industrial e de outras hipóteses de sigilo que sejam essenciais para assegurar os fundamentos do art. 2º do mesmo normativo (ver art. 55-J, II, da LGPD). Ademais, conforme visto no presente caso, o não compartilhamento de informações com esta Autoridade impediu a apreciação de provas que, talvez, pudessem esclarecer as questões levantadas no item [7.48] e a conclusão delineada no item [7.49].

7.55. O compartilhamento de informações com a ANPD poderia ensejar uma atuação diversa da Autoridade, já que, uma vez conhecida a real causa da falha de segurança, seria possível adotar medidas corretivas em primeiro lugar, por meio das quais o regulado seria reconduzido à conformidade, em trabalho colaborativo com a ANPD. Ademais, seria possível até mesmo afastar a violação ao art. 49, da LGPD. Isso, pois, conforme já elucidado pela ANPD em outra ocasião, um incidente de segurança é um evento ao qual todos estão sujeitos, não se tratando de uma questão de "se", mas "quando" vai acontecer[15]. Justamente por isso, cabe à ANPD compreender, mediante a colaboração do agente, sobre as reais causas do incidente, a fim de encará-las como situações às quais o agente de tratamento poderia ter evitado ou não. Neste sentido, as parcas informações apresentadas pela autuada – mesmo após diligenciada a apresentar elementos adicionais – impediram a CGF de avaliar as medidas técnicas adequadas e suficientes para prevenir o incidente e mitigar os seus efeitos, de compreender o momento de ocorrência do incidente e sua causa raiz e, principalmente, de afastar o pressuposto, corroborado nos elementos mínimos do incidente, de que este ocorreu em razão de requisitos de segurança do sistema.

7.56. Importante ressaltar que os agentes de tratamento devem adotar uma postura proativa para a mitigação da ocorrência de tais eventos adversos, a fim de estarem aptos a combatê-los. A título exemplificativo, poderiam ter sido apresentadas medidas de segurança para além das indicadas pela autuada - "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX." (0042386) -, caso fossem consideradas compatíveis à atividade da autuada, como: i) ferramentas de detecção de invasões, com a instalação de firewalls; ii) testes de vulnerabilidade; iii) mecanismos de monitoramento e guarda de registros de acesso à base, aos servidores e por meio da própria aplicação web; ou iv) evidências de não alteração indevida de dados nas bases de dados. [ACESSO RESTRITO - medidas de segurança implementadas em sistema].

7.57. Para fins orientativos, destaca-se que as medidas administrativas se complementam às medidas tomadas para a adequação das estruturas de sistemas utilizados no tratamento de dados[16]. Porquanto determinadas providências tecnológicas não são efetivas quando da ausência de treinamentos para seu uso, assim como capacitações para o devido manejo de dados sem o apoio de tecnologias mínimas de segurança são ineficazes, é de fundamental importância que medidas de segurança técnicas e administrativas em sistemas ou fora deles sejam implementadas de forma harmoniosa. Diante disso, também se estimula a adoção de medidas administrativas junto às organizações, como a própria SAS, apropriadamente, dispôs-se a tomar, consoante trazido em sede de Defesa Administrativa (0050475), com a implementação de eventuais boas práticas e políticas de governança suscitadas na Nota de Esclarecimento (0050478).

7.58. Sob tal perspectiva, a fim de estimular a cultura de proteção de dados alinhada ao princípio da segurança (art. 6º, VII, da LGPD) e ao viés orientativo da Autoridade (art. 29, I, do Regulamento de Fiscalização), a ANPD elaborou o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte[17], cujo conteúdo perpassa por diversas sugestões de medidas de segurança da informação, incluídas medidas administrativas e técnicas que podem servir como orientação para organizações que não restritas às de pequeno porte, ainda que seu foco principal seja para ATPPs.

7.59. Na hipótese de que os sistemas fossem estruturados de maneira adequada antes do incidente, é razoável presumir que as evidências seriam apresentadas desde o primeiro momento em que foram requeridas no processo anterior a este PAS, ou nas duas oportunidades de manifestação (defesa e alegações finais) já no andamento do presente processo sancionador. A apresentação de tais evidências está em consonância com os próprios princípios da *segurança* e da *responsabilização e prestação de contas*, nos termos do art. 6º, VII e X, da LGPD. É oportuno citar, ainda, que desses princípios decorrem também a obrigação de proteger tais dados e a obrigação de demonstrar que estão protegidos.

7.60. Nesse sentido, leciona Miriam Wimmer sobre o princípio da segurança e da prevenção:

> No que tange especificamente aos princípios da segurança e da prevenção, interessa observar que, nos termos do art. 44 da LGPD, **o tratamento de dados pessoais é considerado irregular quando não fornecer a segurança que o titular dele pode esperar**, considerando, dentre outros aspectos, o resultado e os riscos que razoavelmente dele se esperam. A legislação deixa claro, também, que dos agentes de tratamento de dados pessoais é esperada a adoção tanto de

> medidas técnicas como de medidas administrativas para proteger os dados pessoais. Nessa linha, ganha importância a ideia de privacy by design, também prevista na LGPD, que estabelece que as medidas técnicas e administrativas de segurança devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (Grifamos)

7.61. É importante complementar a análise do compromisso do controlador com o que dispõe o princípio da responsabilização e prestação de contas. Novamente, recorre-se à lição de Miriam Wimmer:

> Merece também exame mais aprofundado o princípio da "responsabilização e da prestação de contas" (...).
> Apesar de sua relativa imprecisão conceitual e da dificuldade de traduzir o termo para outros idiomas, trata-se de ideia frequentemente associada à ideia de regulação responsiva ou de corregulação, e, ainda, à noção de uma abordagem baseada em riscos (risk-based approach), **uma vez que atribui ao próprio agente regulado a responsabilidade por adotar e demonstrar a efetividade de medidas técnicas e organizacionais para prevenir eventuais tratamentos irregulares**. (Grifamos)

7.62. Verifica-se, portanto, **a violação ao art. 49 da LGPD, uma vez que não foram adotadas medidas suficientes para garantir a adequada estrutura dos sistemas utilizados no tratamento dos dados pessoais dos titulares.**

Classificação da infração

7.63. É dever dos agentes de tratamento utilizar sistemas para tratamento de dados pessoais que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios da LGPD e às normas regulamentares.

7.64. Considerando o supracitado, percebe-se que os sistemas da SAS não continham proteções bastantes que estivessem alinhadas a efetiva segurança dos dados pessoais, conforme demonstrado nos itens [7.44] a [7.62].

7.65. Segundo prevê o Regulamento de Dosimetria, a infração pode ser considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares. A ausência de medidas suficientes a proteger os dados do titular pode ser classificada como média sob três aspectos, nos termos do art. 8º, §2º, do Regulamento de Dosimetria.

7.66. Em primeiro lugar, o incidente ocorrido i) resultou na exposição de dados pessoais em espaço sem o devido controle de acesso; e ii) permitiu que terceiros pudessem acessar um volume considerável de dados relativos a cada um dos usuários considerados individualmente, ainda que a quantidade de titulares afetados como um todo não tenha sido tão expressivo.

7.67. Em segundo lugar, a eventual atividade de tratamento decorrente do incidente pode impedir ou limitar que os usuários tenham garantido seu direito de acesso ao programa de concessão de gratuidade em transportes intermunicipais, caso seus dados sejam, por exemplo, duplicados e utilizados por terceiros para o uso do mesmo serviço, impedindo o uso pelo verdadeiro titular, o que limitaria o exercício do direito de livre locomoção, capaz de causar danos materiais aos titulares.

7.68. Em terceiro lugar, intimamente atrelado aos parâmetros anteriores, os dados expostos no caso concreto (tipo de deficiência, nome da mãe, e-mail, cópia de foto, cópia de RG, cópia de CPF, cópia de endereço, laudo médico padrão, cópia RG do responsável, cópia CPF do responsável e foto de cartão "VEM LIVRE ACESSO") permitem que o titular possa sofrer danos em situações, por exemplo, de discriminação, violação à imagem, perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos. Isso é especialmente relevante ao ponderar-se que a conjugação de múltiplos dados relativos a uma mesma pessoa pode facilitar que mais ações de fraudes possam ser efetuadas em seu nome, além de conferir maior plausibilidade de que o terceiro seja reconhecido como o verdadeiro titular dos dados expostos.

7.69. Portanto, a falta de cuidado no desenvolvimento de um sistema adequado aos requisitos exigidos pela LGPD permitiu que o incidente ocorresse, oportunizando a potencial ocorrência de afetação dos interesses e direitos fundamentais dos titulares de forma significativa.

7.70. Conclui-se que os requisitos previstos no art. 8º, §2º, do Regulamento de Dosimetria são verificados na infração ao art. 49, da LGPD ora analisada, para ser classificada como média.

7.71. Por fim, no presente caso, a infração versa sobre dados sensíveis (tipo de deficiência e diagnóstico médico) e crianças e adolescentes (consoante relatado no Formulário de CIS [0042386]). Essas características elevam o grau de classificação da infração que, por esse motivo, **passa a ser considerada como grave, segundo art. 8º, §3º, "d", do Regulamento de Dosimetria**[18].

Definição do tipo de sanção administrativa

7.72. Para a definição do tipo de sanção adequada, o art. 9º do Regulamento de Dosimetria, indica que a sanção de advertência pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medidas corretivas. Esta hipótese se aplica à presente infração, tendo em vista a necessidade de impor à infratora medidas corretivas frente à ausência de adequação da estrutura de seus sistemas aos ditames do art. 49, da LGPD.

7.73. Diante disso, impõe-se a seguinte **medida corretiva**:

> a) comprovação da implementação, na estrutura dos sistemas, de medidas técnicas (e administrativas, se aplicável) que já tenham sido realizadas, incluindo aquelas referentes i) à existência de mecanismos de monitoramento de tráfego à base de dados, ii) à guarda de registros de acesso à referida base de dados, e iii) ao acesso restrito ao link que contém a base de dados em discussão, a fim de atestar que sua consulta somente pode ser realizada mediante uso de senha, com nova etapa de identificação, bem como com limitação de acesso para pessoa em nível gerencial (consoante relatado pela própria autuada na CIS [0042386]); assim como outras medidas que a SAS entenda ser cabível.
>
> i. A comprovação dos elementos supracitados no item [7.73], a), caput, pode ser realizada através de declaração assinada pelo Secretário da Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS).
>
> ii. A fim de se comprovar o cumprimento da medida corretiva, determina-se à SAS que junte aos autos, **no**

prazo de 20 (vinte) dias úteis da data de intimação da decisão deste PAS, comprovação de implementação das providências indicadas nesta medida corretiva, que poderá ser realizada por meio da declaração mencionada no item [7.73], a), "i".

7.74. **Subsidiariamente**, impõe-se a seguinte **medida corretiva**:

a) apresentação de um cronograma para a implementação das medidas do item [7.73], a), caput, com a especificação das etapas a serem adotadas.

i. A fim de se comprovar o cumprimento das medidas corretivas, determina-se à SAS que junte aos autos, **no prazo de 20 (vinte) dias úteis** da data de intimação da decisão deste PAS, i) documento (e.g. planilha, documento escrito de forma digital, apresentação de slides etc.) em que conste a previsão de todas as etapas de efetuação do cronograma e ii) a forma por meio da qual se comprovará o cumprimento de cada uma das etapas.

ii. O prazo de cumprimento de todas as etapas previstas no cronograma não deverá ultrapassar 90 (noventa) dias úteis, contados após o transcurso do prazo de 20 (vinte) dias úteis da data de intimação da decisão deste PAS supracitada no item "i".

Adoção de medidas para adequação à LGPD

7.75. Assinala-se que, conforme indicado na Nota de Esclarecimento (0050478), a autuada informou que estabeleceria prazo interno i) "para capacitação da equipe da Secretaria Executiva de Segmentos Sociais (Seses) sobre a importância da implantação do LGPD no tratamento de dados pessoais dos beneficiários dos programas de assistência social sob sua responsabilidade, conforme cronograma de cursos oferecidos pelo Centro de Formação dos Servidores e Empregados Públicos do Estado de Pernambuco (Cefospe)"; ii) "para início da campanha de conscientização quanto ao uso responsável da informação e tratamento de dados, até 31/12/2022" e iii) para a "confecção de Relatório Interno de Impacto a Proteção de Dados Pessoais, até 30/08/2022, para avaliação, dentre outros, da natureza, categoria e quantidade de titulares afetados e das consequências concretas e prováveis".

7.76. Em razão das medidas que foram apontadas pela regulada no sentido de adequar o tratamento de dados pessoais à LGPD, conforme relatado na Defesa Administrativa (0050475), consideram-se ausentes a conveniência e oportunidade de encaminhar notícia ao órgão de controle interno da autuada para apuração de eventual falta funcional, nos termos do art. 55-J, XXII, da LGPD.

8. CONCLUSÃO

8.1. Ante o exposto, considerando que o conjunto probatório demonstra que a autoria e a materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração nº 11/2022/CGF/ANPD (0050468), conclui-se pelas seguintes recomendações:

8.1.1. Por violação ao art. 48 da LGPD, a aplicação da sanção de ADVERTÊNCIA à SAS, com a imposição das seguintes medidas corretivas, acompanhadas de suas comprovações:

a) envio de comunicação direta e individualizada a cada um dos 413 titulares afetados pela exposição dos dados no sítio eletrônico da SAS. A proporcionalidade desta medida decorre do fato de que a SAS sujeita o próprio cadastro dos titulares no programa à submissão de seus respectivos e-mails e endereços físicos.

i. O teor da comunicação individual poderá ser o mesmo da segunda versão da Nota de Esclarecimento (0050478), desde que: i) sejam incluídos os motivos da demora da comunicação, por não ter sido imediata, consoante art. 48, §1º, V, da LGPD; ii) sejam alteradas as informações eventualmente desatualizadas, como, por exemplo, os dados do encarregado e o que mais a SAS entender necessário.

ii. A fim de se comprovar o cumprimento da medida corretiva, determina-se à SAS que junte aos autos, **no prazo de 20 (vinte) dias úteis** contados nos termos do art. 12, I, do Regulamento de Fiscalização, comprovação de que a medida corretiva "a)" descrita no item [8.1.1] foi cumprida por meio da apresentação de uma planilha com a lista completa de todos os 413 titulares afetados identificados que foram individualmente comunicados contendo (i) o nome completo do titular; (ii) data de contato; (iii) informação de contato utilizada para a comunicação individual (o número de telefone, se por meio telefônico; o e-mail, se por correio eletrônico; o endereço, se por meio físico etc); e iv) o envio do inteiro teor de 40 comunicações realizadas por e-mail ou por meio físico, a fim de que seja possível que a CGF valide, por amostragem, a comunicação feita ao titular.

b) atualização da CIS geral no sítio eletrônico da SAS, conforme segunda versão juntada aos autos (0050478), incluídas as alterações mencionadas no item [8.1.1], alínea "a)", primeira subalínea "i", na página em que os usuários se cadastram no Programa PE Livre Acesso (https://www.sdscjpvd.pe.gov.br/seses/pe-livre-acesso-intermunicipal/ ou correspondente), bem como na página específica relacionada à LGPD (https://www.sas.pe.gov.br/lgpd/ ou correspondente), e sua manutenção, por pelo menos mais 90 (noventa) dias corridos a contar da data da intimação da decisão deste PAS. Essa medida é importante para que os titulares tenham mais um veículo de comunicação para tomar ciência do incidente em questão e buscar mais informações junto à SAS.

i. Deverá ser juntada aos autos comprovação de que a medida corretiva do item [8.1.1] "b)" foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela de cada um dos sítios eletrônicos acima indicados da SAS contendo o comunicado e com

visualização clara da data da captura, sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma.

ii. A comprovação de cumprimento da medida corretiva deverá ser juntada aos autos em até 5 (cinco) dias úteis do final de cada período de 30 (trinta) dias, independentemente de nova intimação para tanto.

8.1.2. Por violação ao art. 49 da LGPD, a aplicação da sanção de ADVERTÊNCIA à SAS, com a imposição da seguinte medida corretiva, acompanhada de sua comprovação:

a) comprovação da implementação, na estrutura dos sistemas, de medidas técnicas (e administrativas, se aplicável) que já tenham sido realizadas, incluindo aquelas referentes i) à existência de mecanismos de monitoramento de tráfego à base de dados, ii) à guarda de registros de acesso à referida base de dados, e iii) ao acesso restrito ao link que contém a base de dados em discussão, a fim de atestar que sua consulta somente pode ser realizada mediante uso de senha, com nova etapa de identificação, bem como com limitação de acesso para pessoa em nível gerencial (consoante relatado pela própria autuada na CIS [0042386]); bem outras medidas que a SAS entenda ser cabível.

i. A comprovação dos elementos supracitados no item [7.73], a), caput, pode ser realizada através de declaração assinada pelo Secretário da Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS).

ii. A fim de se comprovar o cumprimento da medida corretiva, determina-se à SAS que junte aos autos, **no prazo de 20 (vinte) dias úteis** da data de intimação da decisão deste PAS, comprovação de implementação das providências indicadas nesta medida corretiva, que poderá ser realizada por meio da declaração mencionada no item [7.73], a), "i".

8.1.3. **Subsidiariamente**, impõe-se a seguinte **medida corretiva**:

a) apresentação de um cronograma para a implementação das medidas do item [8.1.2], a), caput, com a especificação das etapas a serem adotadas.

i. A fim de se comprovar o cumprimento das medidas corretivas, determina-se à SAS que junte aos autos, **no prazo de 20 (vinte) dias úteis** da data de intimação da decisão deste PAS, i) documento (e.g. planilha, documento escrito de forma digital, apresentação de slides etc.) em que conste a previsão de todas as etapas de efetuação do cronograma e ii) a forma por meio da qual se comprovará o cumprimento de cada uma das etapas.

ii. O prazo de cumprimento de todas as etapas previstas no cronograma não deverá ultrapassar 90 (noventa) dias úteis, contados após o transcurso do prazo de 20 (vinte) dias úteis da data de intimação da decisão deste PAS supracitada no item "i".

8.2. Por fim, é importante registrar que a classificação das infrações, a definição das sanções (inclusos agravantes e atenuantes) e a adoção de medidas corretivas restringem-se às circunstâncias deste caso em concreto. Tais decisões não vinculam, naturalmente, a análise e o posicionamento da CGF em futuros processos sancionadores.

9. ENCAMINHAMENTOS

9.1. O presente Relatório de Instrução deve ser encaminhado ao Coordenador-Geral de Fiscalização para decisão, de acordo com art. 55 do Regulamento de Fiscalização.

9.2. Após proferida a decisão, a autuada deverá ser intimada para cumprimento da sanção e/ou apresentação de recurso, em até 10 dias úteis, em consonância com o art. 58 do Regulamento de Fiscalização.

9.3. A decisão deve ser publicada no DOU, segundo o art. 55 do Regulamento de Fiscalização.

9.4. Após trânsito em julgado, este Processo Administrativo Sancionador deverá ser encaminhado para a fase de cumprimento da decisão para acompanhamento das obrigações de fazer determinadas.

À consideração superior.

GABRIELLA VIEIRA OLIVEIRA GONÇALVES
Especialista em Politicas Públicas e Gestão Governamental

De acordo. Encaminhe-se.

ULLIANA CERVIGNI MARTINELLI
Coordenadora de Fiscalização, Substituta

---

[1] Este Relatório de Instrução foi elaborado com a colaboração de Sayuri Pacheco Hamaoka, assistente desta Coordenação-Geral de Fiscalização.
[2] Conforme publicizado no site da Secretaria. Disponível em: https://www.sas.pe.gov.br/wp-content/uploads/2023/12/PORTARIA-SDSCJPVD-n%C2%BA280-2023-Encarregado-LGPD_c%C3%B3pia.pdf. Acesso em 17 abr 2024.
[3] De acordo com o informado no Portal da Lei de Acesso à Informação do Governo de Pernambuco. Disponível em: https://www.lai.pe.gov.br/sdscj-/protecao-de-dados-pessoais/. Acesso em 17 abr 2024.
[4] Conforme denominação dada pela lei nº 16.520, de 27 de dezembro de 2018, revogada pela Lei nº 18.139, de 18 de janeiro de 2023.
[5] Conforme denominação dada pela Lei nº 18.139, de 18 de janeiro de 2023, alterada pela Lei nº 18.487, de 9 de janeiro de 2024.
[6] Como será exposto ao longo deste Relatório de Instrução, observou-se que a quantidade de titulares informada pela SAS que teria sido impactada no incidente variou entre 412 e 413 titulares (Vide: 413 titulares – 0042386; 0050475; e 412 titulares - 0042409; 0042412; 0050479; 0050478).
[7] No decorrer do Processo de Comunicação de Incidente de Segurança nº 00261.001037/2022-06 e no presente Processo Sancionador nº 00261.001963/2022-73, este Despacho foi referenciado pelo SEI nº 3381298. Com a migração dos processos da ANPD ao sistema próprio, o referido documento passará a ser indicado pelo SEI nº 0042390.
[8] A título de esclarecimento, elucida-se que os atos processuais que ensejaram a instauração do presente PAS nº 00261.001963/2022-73 foram praticados no âmbito do Processo de CIS nº 00261.001037/2022-06.
[9] Essencial ressaltar que, ainda que a comunicação geral fosse considerada suficiente neste caso – hipótese aqui

levantada apenas a título explicativo e com propósitos educativos –, a versão mais completa desse comunicado, consubstanciado na Nota de Esclarecimento atualizada constante no site, somente ocorreu após decorrido mais de quatro meses da primeira determinação de que o comunicado fosse emitido (o primeiro pedido foi realizado por meio do Despacho [0042390], expedido em 02/06/2022, conforme indicado no item [5.7]; a Nota de Esclarecimento atualizada, por sua vez, foi apresentada à ANPD no mês de novembro, segundo item [5.22]. Por mais que não haja norma geral e abstrata a respeito, no caso concreto, a CGF indicou reiteradamente o prazo que seria razoável para realizar a comunicação do incidente aos titulares (itens [5.7], [5.8], [5.9], [5.10], [5.13]). Os quatros meses decorridos, portanto, seriam irrazoáveis, diante da demora em face dos seguidos pedidos da CGF à autuada. Julgados nesse sentido constam nos Relatórios de Instrução nº 2/2023, nº 4/2023 e nº 2/2024, respectivamente nos processos 00261.001969/2022-41, 00261.001886/2022-51 e 00261.001192/2022-14.

[10] Disponível em: https://www.sas.pe.gov.br/seses/cadastro-pe-livre-acesso-intermunicipal/. Acesso em: 17 abr 2024.

[11] Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 17 abr 2024.

[12] Julgados neste sentido constam nos Relatórios de Instrução nº 2/2023, nº 4/2023 e nº 2/2024, respectivamente nos processos 00261.001969/2022-41, 00261.001886/2022-51 e 00261.001192/2022-14.

[13] Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 17 abr 2024.

[14] Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 17 abr 2024.

[15] WIMMER, Miriam. Sanções aplicadas pela Autoridade Nacional de Proteção de Dados. Anexo II, Plenário 08: Câmara dos Deputados, 12 abr. 2023. 1 vídeo (4min). Disponível em: https://www.camara.leg.br/evento-legislativo/67461?a=560242&t=1681309481253&trechosOrador=&crawl=no. Acesso em 14 mar 2024.

[16] Por este ponto de vista: "Nesse sentido, a segurança que se espera não é aplicada exatamente aos dados em si, mas sim aos sistemas que os mantêm (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Isso significa que não bastam as medidas técnicas, como o uso de firewalls, métodos criptográficos e controles de conteúdo, se elas não vierem acompanhadas de outras medidas, como treinamentos de segurança, criação de políticas de segurança da informação, inventários de ativos etc.". MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. In: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2023, p. 348.

[17] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 17 abr 2024.

[18] Julgados neste sentido constam nos Relatórios de Instrução nº 2/2023, nº 4/2023 e nº 2/2024, respectivamente nos processos 00261.001969/2022-41, 00261.001886/2022-51 e 00261.001192/2022-14.

Documento assinado eletronicamente por **Ulliana Cervigni Martinelli**, **Coordenador(a), Substituto(a)**, em 25/04/2024, às 15:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Gabriella Vieira Oliveira Goncalves**, **Especialista em Políticas Públicas e Gestão Governamental - EPPGG**, em 25/04/2024, às 15:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0117502** e o código CRC **C74A7EB6**.