



CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA
RUA RODRIGUES DE AQUINO, nº 208 – CENTRO | João Pessoa – PB | CEP 58015-040
Nome do Encarregado de Proteção de Dados: DEGINALDA FABIA BARBOZA MENDES

Relatório de Impacto de Proteção de Dados

Para atendimento aos art. 10, §3º e 38 da Lei 13.709/2018

RH - Atestados e declarações médicas

Situação do RIPD: Aprovado

Versão: 1

Aprovado em: 27/01/2025 10:12:11 por Fabia Barboza Mendes

Dados do Controlador:

Nome/Razão Social: CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA
Pessoa de Contato: Abelci Daniel de Assis Filho
Cargo/Função:
Endereço completo: RUA RODRIGUES DE AQUINO
CEP: 58015-040
Cidade: João Pessoa
UF: PB
Telefone: (83) 3044-1313
E-mail: governanca@crcpb.org.br
Site: https://crcpb.org.br/

Dados do Encarregado de Proteção de Dados:

Nome: DEGINALDA FABIA BARBOZA MENDES
Cargo/Função:
Telefone: (83) 3044-1313
E-mail: diretoria@crcpb.org.br

Atividade de Processamento de Dados

Atividade

Departamentos Responsável

- Recursos Humanos (Setor Contábil/Financeiro)

Pessoa Responsável/Cargo

Sr Alex Barros/Coordenador(a) do Recursos Humanos

Objetivo da Atividade de Processamento

Quando o servidor faz o encaminhamento e consultas, em alguns casos, disponibiliza previamente por e-mail e entrega fisicamente quando retorna as atividades. O setor, então, recebe o atestado e armazena em pasta individuais de cada servidor. Com o documento em mãos, coloca as informações (tempo de afastamento, CID, nome do médico, CRM do médico) no sistema Domínio. Automaticamente, o sistema Domínio integra as informações no E-social. Com o recebimento do atestado/declaração médica, as ausências são registradas e abonadas no sistema VM Ponto pelo setor de Tesouraria [Processo é finalizado].

Método de Coleta dos Dados

Titular disponibiliza o atestado fisicamente

Observações

1. Sugerir um e-mail específico para RH/DP/GP. 2. O sistema Domínio trata dados pessoais sensíveis, atenção na revisão de contratos.

Base Legal para atividade de Processamento

| Base Legal | Referência em Lei | Descritivo Técnico |
|--|-------------------|--|
| Cumprimento de Obrigação Legal ou Regulatória pelo Controlador | Art. 7, II, LGPD. | Conforme determina o Art. 7º, inciso II da LGPD: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: para o cumprimento de obrigação legal ou regulatória pelo controlador. Portanto, em se tratando de um processo administrativo pelo CRC/PB, a base legal mais adequada para esta atividade de processamento é esta. |

Justificativa do Uso da Base Legal

Conforme determina o Art. 7º, inciso II da LGPD: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: para o cumprimento de obrigação legal ou regulatória pelo controlador. Portanto, em se tratando de um processo administrativo pelo CRC/PB, a base legal mais adequada para esta atividade de processamento é esta.

Conjunto de dados utilizados na atividade

Atestado

Atestado

| Dado | Titular | Sensibilidade | Descritivo |
|--|-------------|---------------|--|
| Nome do médico | Colaborador | Não | Nome do médico |
| Tempo de afastamento | Colaborador | Não | Tempo de afastamento |
| CID - Classificação Internacional de Doenças | Colaborador | Sim | CID - Classificação Internacional de Doenças |
| Informações de Saúde | Colaborador | Sim | Tipo sanguíneo, doador de órgãos e tecidos. |
| CRM do médico | Colaborador | Não | CRM do médico |

Trata Dados de Criança e/ou Adolescente?

Não

Categorias de titulares de dados atingidos pela atividade de processamento

| Titular | Descritivo |
|-------------|-------------|
| Colaborador | Colaborador |

Legislação e Sistema de Armazenamento

Legislação: Decreto - Lei - Getúlio Vargas (Presidente da República) - 5452 - Decreto - Lei N° 5.452/43 - 01/05/1943

Sistemas de Armazenamento:

- Pastas Digitais (Financeiro)
- Pastas Físicas (Financeiro)

DFB Mendes

DFB/ends



DTB/mde



DFB Mendes



Acesso Externo: - Pastas Digitais (Financeiro)
 Não
 - Pastas Físicas (Financeiro)
 Não

Tempo de Processamento/Manutenção: - **Conjunto de Dados:** Atestado
 - **Tempo Legal de Processamento:** Não definido
 - **Método de Descarte:** Não definido

Transferência para Terceiro/Operador

| Razão Social + CNPJ | Finalidade da transferência | Método da Transferência | Transferência Internacional | Controlador Conjunto |
|---|--------------------------------------|-------------------------|-----------------------------|----------------------|
| E-social | Integração de dados | Via sistema | NÃO | NÃO |
| DOMINIO SISTEMAS E SERVICOS DE INFORMATICA LTDA | Inserção e armazenamento do atestado | Via sistema | NÃO | NÃO |
| VM ponto | Registro e abono de atestado médico | Via sistema | NÃO | NÃO |

Handwritten signature

Handwritten signature

Questões

GRUPO – AVALIAÇÃO

Como os titulares dos dados são informados sobre o tratamento dos seus dados?

Justificativa: No momento da entrega do atestado físico ao setor responsável.

Como é obtido o consentimento dos titulares de dados?

Justificativa: Não há consentimento do titular nesta atividade pela base legal ser outra.

Como é garantido o acesso e portabilidade de dados pessoais?

Justificativa: Após incluso os dados no sistema Domínio, o titular pode acessar e verificar se os dados foram inseridos de forma correta.

Como é garantida a atualização/retificação e a exclusão dos dados pessoais solicitada pelo titular dos dados?

Justificativa: O titular pode requerer a atualização/retificação dos dados via e-mail ou presencialmente com o setor responsável.

Como é garantida a limitação do tratamento dos dados pessoais solicitada pelo titular dos dados?

Justificativa: O setor responsável gere a requisição do titular informando sobre os direitos do mesmo via e-mail ou presencialmente no setor.

As obrigações dos subcontratantes são claramente identificadas e reguladas por contrato ou outro ato normativo?

Justificativa: Sim.

No caso de transferência de dados fora do Brasil, os dados são adequadamente protegidos?

Justificativa: Não se aplica.

DFB Mendes



Riscos

DTB Mendes



GRUPO – RISCO

Nome: Necessidade de Verificação de Contrato

Descrição: Necessidade de Verificação de Contrato

Esse risco afeta confidencialidade

Esse risco afeta integridade

Esse risco afeta disponibilidade

Quais são os principais impactos nos dados dos titulares se o risco ocorrer?

Justificativa: Vazamento indevido dos dados abordados.

Quais são os principais ameaças que poderiam levar ao risco?

Justificativa: A falta de treinamento devido para lidar com os dados abordados em contrato.

Quais são as fontes de risco?

Justificativa: A necessidade de verificação de contrato para compartilhamento com o sistema.

Como você avalia o impacto do risco, especialmente de acordo com impactos potenciais e controles planejados?

Impacto Alto

Justificativa: Por envolver dados sensíveis.

Como estimas a probabilidade de risco, especialmente em relação a ameaças, fontes de risco e controles planejados?

Probabilidade Alto

Justificativa: Devido a necessidade de revisão de contrato.

Pontuação Muito Alto

Conduta de Mitigação: Inserir Cláusulas de Segurança e Privacidade

Como: (i) Incluir cláusulas de segurança da informação que detalhem as medidas de proteção que uma contratada deve adotar para evitar vazamentos.

GRUPO – RISCO

Nome: Vazamento de Dados por Envio de E-mails Não Seguros

Descrição: Dados pessoais podem ser expostos em e-mails enviados sem criptografia.

Esse risco afeta confidencialidade

Esse risco afeta disponibilidade

Quais são os principais impactos nos dados dos titulares se o risco ocorrer?

Justificativa: Informações confidenciais serem acessadas por terceiros durante a transmissão.

Quais são os principais ameaças que poderiam levar ao risco?

Justificativa: A falta de gerenciamento de e-mails seguros.

Quais são as fontes de risco?

Justificativa: A ausência de criptografia no envio de e-mails para o sistema.

Como você avalia o impacto do risco, especialmente de acordo com impactos potenciais e controles planejados?

Impacto Alto

Justificativa: Devido a lidar com dados sensíveis.

Como estimas a probabilidade de risco, especialmente em relação a ameaças, fontes de risco e controles planejados?

Probabilidade Alto

Justificativa: Devido a ausência de criptografia para envio de dados.

DFB Mendes



Pontuação Muito Alto

Conduta de Mitigação: Uso de Criptografia no Envio de E-mails

Como: (i) Utilizar e-mails criptografados e plataformas seguras para envio de documentos; e (ii) Treinar funcionários para evitar envio de dados pessoais por e-mails não autorizados.



| | | | | | | |
|---------|---------------|-------------|-------------|-------------|------------|------------|
| IMPACTO | Muito Alto | Médio | Alto | Muito Alto | Muito Alto | Muito Alto |
| | Alto | Baixo | Médio | Alto | Muito Alto | Muito Alto |
| | Médio | Muito Baixo | Baixo | Médio | Alto | Muito Alto |
| | Baixo | Muito Baixo | Muito Baixo | Baixo | Médio | Alto |
| | Muito Baixo | Muito Baixo | Muito Baixo | Muito Baixo | Baixo | Médio |
| | Muito Baixo | Baixo | Médio | Alto | Muito Alto | |
| | PROBABILIDADE | | | | | |

DFB Mendes

Parecer Técnico

Parecer Técnico - Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD)

1. Contextualização

Este parecer tem como objetivo analisar o fluxo de tratamento de dados pessoais sensíveis no processo de encaminhamento de atestados e registros de ausência de servidores, conforme descrito, em relação às obrigações da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

2. Análise do Fluxo

O processo envolve as seguintes etapas:

- Recebimento de atestado médico** : O servidor encaminha o atestado por e-mail e a entrega fisicamente ao retorno às atividades.
- Armazenamento de documentos** : O setor responsável recebe o atestado e o armazena em pastas individuais.
- Registro de informações no sistema Domínio** : São inseridas informações como tempo de afastamento, CID (Classificação Internacional de Doenças), nome do médico e CRM.
- Integração ao E-social** : As informações são automaticamente fornecidas pelo sistema Domínio para o E-social.
- Registro e abono de ausências** : A Tesouraria registra e abona as ausências no sistema VM Ponto, finalizando o processo.

3. Conformidade com a LGPD

Para verificar a adequação deste fluxo à LGPD, é necessário analisar alguns pontos-chave:

um. Base Legal para o Tratamento de Dados

Os dados sensíveis envolvidos (como informações de saúde) necessitam de uma base legal robusta. Neste caso, o tratamento dos dados é necessário para o cumprimento de obrigação legal ou regulatória pelo controlador, conforme artigo 11, inciso II, cláusula 'a', da LGPD.

b. Finalidade, Necessidade e Adequação

O tratamento de dados pessoais deve observar os princípios da especificamente, necessidade e adequação (art. 6º, incisos I, II e III):

- Finalidade** : Os dados são tratados para uma finalidade específica e legítima: o registro de ausências e o encaminhamento de informações ao E-social.
- Necessidade** : As informações coletadas (tempo de afastamento, CID, nome do médico e CRM) são essenciais para o processo de abono de faltas e cumprimento de obrigações trabalhistas.
- Adequação** : O tratamento é adequado, pois o sistema Domínio foi escolhido como ferramenta para inserção e integração dos dados com o E-social.

c. Segurança e Armazenamento de Dados

A LGPD exige que os dados sejam armazenados de forma segura (art. 6º, inciso VII). Recomenda-se verificar se as massas físicas são mantidas em local seguro e de acesso restrito. Além disso, o sistema Domínio deve possuir medidas técnicas e administrativas para garantir a integridade, confidencialidade e disponibilidade das informações.

d. Compartilhamento de Dados

O compartilhamento de dados com o E-social faz parte do cumprimento de obrigações legais. No entanto, é crucial que o compartilhamento seja restrito ao mínimo necessário e siga os princípios da LGPD, garantindo que apenas os dados pertinentes ao objetivo sejam transferidos.

e. Transparência e Direito dos Titulares

Os servidores devem ser informados sobre o tratamento de seus dados (art. 9º). Isso detalha sobre a coleta, processamento, tempo de retenção e compartilhamento de dados com o E-social, além de permitir o exercício dos direitos previstos na LGPD, como acesso, correção e revogação de consentimento (art. 18).

4. Recomendações

- Elaboração de Política de Privacidade Interna** : É importante possuir uma política clara sobre o tratamento de médicos atestados, com base específica, bases legais e procedimentos de segurança.
- Armazenamento Seguro** : Manter as pastas físicas em local seguro, com acesso restrito, e garantir que o sistema Domínio tenha medidas adequadas de segurança cibernética.
- Treinamento de Pessoal** : Oferece treinamento aos colaboradores envolvidos no tratamento de dados sensíveis para segurança as práticas de segurança e privacidade.
- Gestão de Consentimento e Transparência** : Garantir que os servidores sejam informados sobre o tratamento de seus dados e possam exercer seus direitos em conformidade com a LGPD.

5. Conclusão

O fluxo descrito apresenta conformidade com a LGPD, especialmente no que diz respeito à base legal para o tratamento de dados pessoais, ao cumprimento de obrigações trabalhistas e à transparência. No entanto, a implementação de práticas de segurança e treinamentos adicionais são fundamentais para fortalecer a proteção dos dados dos servidores e garantir a conformidade plena com a legislação.

Este parecer técnico visa orientar sobre as boas práticas e a adequação à LGPD no processo de registro e encaminhamento de atestados médicos, garantindo o cumprimento dos direitos dos titulares e a segurança dos dados protegidos tratados.

João Pessoa, 27/01/2025 10:12:11



DEGINALDA FABIA BARBOZA MENDES
CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA



Abelci Daniel de Assis Filho
CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA

DTB/Ends
