DOCUMENTAÇÃO CONTROLADA

POLÍTICA GERAL DE PRIVACIDADE DE DADOS

PROCEDIMENTO : PG-CPD-001-21

HyonPar

SUMÁRIO

VERSÃO	DATA	RESPONSÁVEL	RESUMO ALTERAÇÃO
00	28/06/2021	Victor Rizzo	Elaboração inicial do procedimento
01	25/09/2023	Leandro Alves	Inclusão dos itens: 5.8, 5.8.1, 5.8.2, 5.8.3, 5.8.4

1. OBJETIVO

O objetivo desta Política Geral de Privacidade de Dados (PGPD) é o de fornecer as diretrizes para tratamento de dados pessoais para todas as empresas da HYON PAR, doravante referidas como ORGANIZAÇÃO.

A Organização entende que a informação é o ativo mais importante para os nossos negócios. Assim garantir a segurança da informação e a privacidade de dados das empresas do grupo e de seus clientes é um dos principais pilares de nossa governança.

A Organização, através de suas empresas controladas e coligadas, oferece diversos serviços que envolvem o tratamento de dados pessoais e diversos outros dados corporativos.

O tratamento de dados pessoais é parte essencial de todos os negócios da Organização e, portanto, a privacidade de dados pessoais é um elemento essencial para o desempenho e a conformidade dos negócios da mesma.

Além disso, através dessa Política de Privacidade de Dados Pessoais a Organização reconhece sua responsabilidade no tratamento de dados pessoais, e comprometem-se e envidar os esforços administrativos e técnicos necessários para garantir a privacidade e os direitos de pessoas naturais, com as quais a Organização tenham relações direta ou indiretamente.

Neste sentido, a Organização, possui sistemas, sites digitais, canais de comunicação nas redes sociais, documentos, dentre outros, por meio dos quais são realizados o tratamento de dados pessoais de clientes ou partes interessadas.

A presente Política de Privacidade de Dados Pessoais tem como objetivo fornecer as diretrizes para o tratamento de dados pessoais, relacionados às partes interessadas, que assegurem e reforcem o compromisso da Organização com o cumprimento das legislações de proteção de dados pessoais aplicáveis.

Este documento se insere no Programa de Conformidade da HYON PAR, à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018. Esta Política, se insere no conjunto de iniciativas que integram as diretrizes e controles para garantia da **Governança Digital e Conformidade da HYON PAR**, e deve ser interpretada e implantada em

conjunto de documentos e normativas que compõem a estrutura de segurança de informação e privacidade de dados da organização.

2. DEFINIÇÕES

Para fins deste procedimento, consideram-se as definições abaixo, tal como estabelecidas no Art. 5º da Lei nº 13.709/2018.

Dado pessoal - informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado anonimizado - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Banco de dados - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular de Dados Pessoais (Titular) - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Agentes de tratamento - o controlador e o operador;

Tratamento de Dados Pessoais (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;

Anonimização - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Consentimento - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio - suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação - exclusão de dado ou de conjunto de dados armazenados em banco de dados, ou em meio físico, independentemente do procedimento empregado;

Transferência internacional de dados - transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Uso compartilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Relatório de impacto à proteção de dados pessoais (RIPD) - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Além destas, consideram-se as seguintes definições:

Cliente da Organização (Cliente) – Pessoa Jurídica ou Física, com a qual uma das empresas da Organização possui relação contratual para prestação de serviços.

Partes interessadas - para o objetivo desta PGPD, pessoas físicas, incluindo colaboradores, sócios, clientes, potenciais clientes, parceiros, fornecedores, consultores, parceiros comerciais, visitantes de sites digitais, escritórios e demais dependências físicas, ou outros tipos de partes interessadas, que de alguma forma estejam envolvidas com as atividades desenvolvidas pelas empresas da Organização.

3. DOCUMENTOS DE REFERÊNCIA

- **Lei nº 13.709/2018** - Lei Geral de Proteção de Dados (LGPD)
- **MQ-CGQ-004-19** - Manual do Sistema de Gestão da Qualidade
- **PO-CGQ-001-18** - Procedimento de Elaboração e Controle de Documento da Qualidade
- **PG-CPD-002-21** - Política de Privacidade de Sistemas
- **PO-CPD-002-21** - Procedimento de Resposta a Solicitação de Titulares
- **PO-CGQ-004-21** - Procedimento de Avaliação de Risco

4. ABRANGÊNCIA

Todas as empresas da Organização

Todas as áreas das empresas

5. DETALHAMENTO

5.1 Generalidades

Todas as empresas da Organização deverão desenvolver programas das Privacidade de Dados Pessoais e adequação à LGPD com base das diretrizes estabelecidas nessa PGPD.

Para a implantação de programas de Privacidade de Dados Pessoais as empresas deverão considerar as seguintes etapas:

a) Planejamento Geral;
b) Nomeação do Encarregado de Dados Pessoais;
c) Treinamento Geral para Equipes (Principais conceitos da LGPD);
d) Diagnóstico de Situação Atual;
e) Levantamento de Fluxo de Dados e Documentos;
f) Planejamento do Tratamento de Dados Pessoais;
g) Análise de Risco de Tratamento de Dados Pessoais;
h) Definição de Processo de Resposta de Solicitações de Titulares e ANPD;
i) Revisão de Contratos de Colaboradores;
j) Revisão de Contratos de Fornecedores;
k) Revisão de Contratos de Clientes;
l) Revisão de Procedimentos Operacionais;
m) Implementação de Políticas de Consentimento;
n) Definição de Plano de Gestão de Incidentes de Vazamentos de Dados;
o) Treinamentos Específicos para Equipes;
p) Adequação de Sistemas e Infraestrutura;
q) Plano de Testes de Segurança de Informação;
r) Elaboração de Relatório de Impacto de Proteção de Dados (RIPD);
s) Definição de Planos de Auditoria Periódica.

5.2 Planejamento Geral

No planejamento geral deverão ser consideradas, as áreas prioritárias para implantação, o método de levantamento, bem como os prazos gerais.

5.3 Nomeação do Encarregado de Dados Pessoais

A nomeação do encarregado de dados deverá ser feita de maneira formal, e a informações de contato desse deverão ser divulgadas nos canais de comunicação da empresa.

São atribuições do Encarregado de Dados Pessoais:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo CONTROLADOR ou estabelecidas em normas complementares.
- Fomentar e disseminar a cultura de privacidade de dados.
- Prestar esclarecimentos aos clientes do CONTROLADOR, sobre as medidas adotadas para a implantação da LGPD

5.4 Treinamento Geral para Equipes (Principais conceitos da LGPD)

Treinamento geral para as equipes das áreas de negócio da empresa, sobre os principais conceitos da LGPD, incluindo minimamente:

- Origens da LGPD;
- Objetivos da LGPD;
- Titular de Dados Pessoais;
- Controlador de Dados;
- Operador de Dados;
- Agência Nacional de Proteção de Dados (ANPD);
- Encarregado de Dados (DPO);
- Dados Pessoais;
- Dados Sensíveis;
- Dados Anonimizados;
- Dados de Crianças e Adolescentes;
- Tratamento de Dados Pessoais;
- Direitos do Titular de Dados;

- Obrigação da Empresa (Controlador ou Operador de Dados);
- Base Legais para o Tratamento de Dados;
- Sanções e Penalidades.

5.5 Diagnóstico de Situação Atual

Diagnóstico, através de check-lists e levantamentos nas áreas de negócio, do atual estado de conformidade com as práticas exigidas pela LGPD.

5.6 Levantamento de Fluxo de Dados e Documentos

Levantamento dos fluxos de dados e documentos que envolvam dados pessoais, identificando os tipos de dados tratados, os repositórios e áreas envolvidas no tratamento de dados.

5.7 Planejamento do Tratamento de Dados Pessoais

Planejamento do tratamento envolvendo as operações realizadas com dados pessoais, incluindo 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.

Todas as etapas de tratamento de dados devem ser realizadas adotando das melhores práticas de segurança de informação necessárias, incluindo medidas administrativas e técnicas, para proteção da privacidade do titular de dados.

Em especial devem ser considerados:

a) Coleta de Dados Pessoais

A coleta de dados de dados pessoais, deverá ser planejada dentro do âmbito de cada um dos produtos ou serviços, considerando a necessidade específica do mesmos, e restringindo o escopo de coleta à demanda dos específica dos produtos ou serviços, e das obrigações contratuais previstas.

Além destes tratamentos de dados, devem ser ainda considerados:

b) Anonimização de dados pessoais

A anonimização de dados pessoais, somente deverá ocorrer em situações específicas:

- Por solicitação expressa do titular dos dados pessoais;
- Por solicitação expressa do cliente;
- Quando o tratamento dos dados pessoais seja desnecessário, excessivo, ou esteja sendo realizado em desconformidade com o disposto na LGPD.

A anonimização de dados somente deverá ocorrer em condições que:

- Seja estritamente necessária;
- Seja tecnicamente viável;
- Não inviabilize a prestação do serviço e o cumprimento das obrigações contratuais com o titular de dados, clientes, fornecedores e parceiros;
- Não inviabilize o cumprimento de obrigações legais ou regulatórias;
- Não inviabilize o regular exercício de direitos da empresa e o atendimento de seus legítimos interesses.

c) Eliminação ou Expurgo de Dados Pessoais

A eliminação ou expurgo de dados pessoais, somente deverá ocorrer em situações específicas:

- Por solicitação expressa do titular dos dados pessoais;
- Por solicitação expressa do cliente;
- Quando o tratamento dos dados pessoais seja desnecessário, excessivo, ou esteja sendo tratado em desconformidade com o disposto na LGPD.
- Após o encerramento da relação contratual com o titular dos dados ou clientes, ressalvados os prazos previstos em lei ou acordados em contratos específicos.

A eliminação ou expurgo de dados somente deverá ocorrer em condições que:

- Seja estritamente necessária;
- Seja tecnicamente viável;
- Não inviabilize a prestação do serviço e o cumprimento das obrigações contratuais com o titular de dados, clientes, fornecedores e parceiros;
- Não inviabilize o cumprimento de obrigações legais ou regulatórias;
- Não inviabilize o regular exercício de direitos da empresa e o atendimento de seus legítimos interesses.

A eliminação ou expurgo de dados pessoais, quando aplicável, deverá ser realizado de acordo com tabelas de temporalidade, de acordo com o tipo de dados pessoal ou documento.

Tabelas de temporalidade específicas poderão ser acordadas com os clientes, dentro do escopo dos respectivos contratos.

A eliminação ou expurgo de dados, deverá ser realizado sempre com as medidas de segurança adequadas, aptas a proteger os dados pessoais de acesso não autorizado.

5.8 Finalidade do Tratamento de Dados Pessoais

5.8.1 Captura de Dados Judiciais Públicos

- Essa coleta possui como finalidade o regular cumprimento de contratos onde nossos clientes, Pessoas Jurídicas, são partes nessas demandas judiciais e controladoras dos dados, estando em conformidade legal conforme artigo 7, IX da Lei Federal 13.709/2018 (Lei Geral de Proteção a Privacidade de Dados Pessoais).

5.8.2 Coleta de Dados Pessoais de Colaboradores

- Essa coleta possui como finalidade o regular cumprimento de contratos de trabalho estando em conformidade legal conforme artigo 7, II da Lei Federal 13.709/2018 (Lei Geral de Proteção a Privacidade de Dados Pessoais).

5.8.3 Coleta de dados pessoais em nosso portal online ou formulários de negócios e Coleta de dados pessoais públicos em redes sociais.

- Essa coleta possui como finalidade o legitimo interesse da empresa em gerar novas oportunidades de negócio, estando em conformidade com o Artigo 7, IX Lei Federal 13.709/2018 (Lei Geral de Proteção à Privacidade de Dados Pessoais).

5.8.4 Coleta de dados pessoais de fornecedores (prestadores de serviços)

- Essa coleta possui como finalidade o legitimo interesse da empresa em gerar novas oportunidades de negócio, estando em conformidade com o Artigo 7, II e V Lei Federal 13.709/2018 (Lei Geral de Proteção à Privacidade de Dados Pessoais).

5.9 Análise de Risco de Tratamento de Dados Pessoais

A análise de risco deverá ser realizada para identificar as etapas do tratamento de dados pessoais que oferecem riscos à privacidade e deverá ser elaborada com base no procedimento **PO-CGQ-004-21** - Procedimento de Avaliação de Risco.

Para os riscos à privacidade de dados considerados relevantes será necessário elaborar um plano de resposta ao risco, com a descrição das medidas de resposta ao risco, conforme estabelecido no procedimento citado.

A análise de risco deverá ser realizada em atividades que envolvam dados pessoais, nas seguintes circunstâncias:

- Em processos de negócio já existentes;
- No desenvolvimento de novos produtos e serviços;
- No desenvolvimento de novas funções de produtos e serviços já existentes.

A análise de risco de privacidade de dados deverá ser revisada anualmente e fim de avaliar a evolução dos riscos.

5.10 Definição de Processo de Resposta de Solicitações de Titulares e ANPD

As empresas deverão definir processo de resposta de solicitações de titulares de dados e da ANPD, de forma a garantir a efetiva resposta, em tempo adequado, às demandas recebidas.

5.11 Revisão de Contratos de Colaboradores

Os contratos de trabalho com colaboradores deverão ser revistos para a inclusão de cláusulas específicas relativas à privacidade de dados, em conformidade com as disposições da LGPD.

5.12 Revisão de Contratos de Fornecedores

Os contratos de fornecedores deverão ser revistos para a inclusão de cláusulas específicas relativas à privacidade de dados, em conformidade com as disposições da LGPD.

5.13 Revisão de Contratos de Clientes

Os contratos de clientes deverão ser revistos para a inclusão de cláusulas específicas relativas à privacidade de dados, em conformidade com as disposições da LGPD.

5.14 Revisão de Procedimentos Operacionais

Os procedimentos operacionais deverão ser revistos para sua adequação e conformidade com as disposições da LGPD.

5.15 Implementação de Políticas de Consentimento

Políticas de consentimento deverão ser implementadas nos canais de comunicação com os clientes.

5.16 Definição de Plano de Gestão de Incidentes de Vazamentos de Dados

As empresas da Organização deverão definir planos de gestão de incidentes de vazamento de dados que contemplem:

- Identificação da origem do vazamento;
- Identificação dos dados vazados;
- Avaliação da criticidade e extensão do vazamento;
- Medidas de contingência para contenção do vazamento de dados;
- Comunicação sobre o vazamento de dados;
- Medidas de correção para a prevenção de vazamentos futuros.

5.17 Treinamentos Específicos para Equipes

As equipes deverão ser treinadas especificamente para os processos e procedimentos revisados.

5.18 Adequação de Sistemas e Infraestrutura

Os sistemas e infraestruturas deverão ser adequados aos requisitos da LPGD e aos riscos identificados na etapa de avaliação de riscos. As principais vulnerabilidades devem ser mapeadas e tratadas, de forma a prevenir vazamentos de dados, intencionais ou acidentais. Os sistemas deverão incorporar melhores práticas de segurança de informação em seu desenvolvimento.

5.19 Plano de Testes de Segurança de Informação

Os sistemas e infraestrutura deverão ser testados. As vulnerabilidades deverão ser exploradas para verificação da sua resiliência à ataques de diversos tipos.

5.20 Elaboração de Relatório de Impacto de Proteção de Dados (RIPD)

Todas as empresas da Organização deverão elaborar os seus Respectivos Relatórios de impactos de Proteção de Dados.

Estes relatórios deverão conter minimamente:

- A identificação dos agentes de tratamento de dados;
- A identificação do encarregado de dados;
- A descrição do escopo de tratamento de dados;
- A descrição da finalidade do tratamento de dados;
- A identificação das partes interessadas no tratamento de dados;
- As diversas etapas de tratamento de dados;
- Os riscos envolvidos no tratamento de dados pessoais;
- O plano de resposta ao risco, com a descrição das respectivas medidas de resposta ao risco;
- As aprovações do relatório.

Os RIPD´s são deverão possuir classificação de segurança de informação “reservado”, conforme estabelecido no procedimento **PO-CGQ-001-18** - Procedimento de Elaboração e Controle de Documento da Qualidade.

A revisão dos RIPD´s deverá ocorrer anualmente, ou sempre que uma alteração significativa seja introduzida no negócio, pelo desenvolvimento de um novo produto ou serviço.

5.21 Definição de Planos de Auditoria Periódica.

Os procedimentos envolvendo a privacidade de dados pessoais deverão ser auditados periodicamente. Planos de auditoria específicos deverão ser desenvolvidos para tal fim, definindo prazos, escopo de auditoria e responsáveis.

5.22 Periodicidade de Revisão da PGPD

Esta política deverá ser revisada anualmente, em conformidade com o procedimento **PO-CGQ-001-18** - Procedimento de Elaboração e Controle de Documento da Qualidade.

6. MATRIZ DE RESPONSABILIDADE

Abaixo encontra-se a disposição das responsabilidades em relação a Política Geral de Privacidade de Dados:

RESPONSÁVEL	ATIVIDADE
Diretoria Executiva	a) Instituir o Comitê de Privacidade de Dados; b) Nomear o Encarregado de Dados Pessoais; c) Disponibilizar os recursos necessários para implantação dessa PGPD d) Disponibilizar os meios, prazos, recursos materiais e humanos necessários e adequados, a fim de que o Encarregado possa desempenhar suas atividades; e) Garantir ao Encarregado a liberdade na realização de suas atribuições; f) Divulgar publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do Controlador, os dados de contato do Encarregado.
Comitê de Privacidade de Dados	a) Elaborar, aprovar e revisar da PGPD; b) Coordenar e suportar a implantação a LGPD nas empresas da Organização; c) Acompanhar o progresso da implantação dessa PGPD e da LGPD nas empresas da Organização; d) Elaborar os procedimentos gerais relacionados à implementação dessa PGPD e da LGPD;

	e) Reunir-se periodicamente para avaliação das práticas de privacidade de dados pessoais nas empresas da Organização; f) Analisar e responder a casos de vazamento de dados.
Encarregado de Dados Pessoais	a) Conforme disposto no item 5.3
Auditoria (quando disponível)	a) Estabelecer os planos de auditoria necessários para garantida da conformidade a essa PGPD e a LGPD; b) Auditar a conformidade de processos e sistemas à LGPD.
Gerentes de Áreas de Negócio	a) Observar essa PGPD e implantar a LGPD em suas respectivas áreas de negócio; b) Revisar procedimentos e sistemas para sua adequação a essa PGPD a LGPD; c) Garantir da conformidade dos processos e sistemas sob sua responsabilidade a essa PGPD e a LPDG;
Coordenadores de Áreas	a) Observar essa PGPD e implantar a LGPD em suas respectivas áreas; b) Garantir da conformidade dos processos e sistemas sob sua responsabilidade a essa PGPD e a LGPD.
Colaboradores	a) Observar essa PGPD e as disposições da LGPD em suas atividades; b) Garantir da conformidade das atividades sob sua responsabilidade à LPDG;

7. REGISTROS DA QUALIDADE

Revisões dentro da periodicidade definida no item 5.20

8. INDICADORES DE DESEMPENHO

Não aplicável

9. CONTROLES DO PROCESSO

Não aplicável

10. ANEXOS

10.1 – FLUXOGRAMA DO PROCESSO

Não aplicável

10.2 – CHECK-LIST

Não aplicável

10.3 – MODELO DE FORMULÁRIO

Não aplicável

10.4 – OUTROS DOCUMENTOS ESPECÍFICOS

Não aplicável