RESPONSÁVEIS	
Ação	**Responsável**

INFORMAÇÕES DO DOCUMENTO				
Código	**Revisão**	**Idioma**	**Data da Revisão**	**Data da Próxima Revisão**
CORP-COM-MA-0001	2		08/05/2026	08/05/2028
Título				
Justificativa da Última Revisão				
Alteração do "Encarregado", indicado nos itens I e V.				

INFORMAÇÕES IMPORTANTES
Toda a documentação do sistema deve ser dinâmica, portanto, passível de comentários e revisões. Sugestões para o aprimoramento devem ser encaminhadas através do módulo Sugestões e Críticas no Sistema Vitora. Em uma nova revisão, sua sugestão será avaliada.

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY

SUMÁRIO

Sumário

I. Apresentação 2
II. Aplicabilidade da LGPD 2
Do que a lei trata? 2
Quando a LGPD é aplicável? 2
III. Conceitos (da LGPD) 3
IV. Princípios 4
V. Autorização de tratamento 4
Solicitação de autorização de uso e compartilhamento dados 4
Modo de solicitação por titulares de dados pessoais 4
Modo de atendimento à solicitação de titulares de dados pessoais 5
VI. Fluxo de dados 5
VII. Classificação de dados 5
Dados pessoais 5
Dados sensíveis 5
Dados sigilosos 5
VIII. Avaliação do risco – matriz risco 6
IX. Cookies 6
Opção quanto aos cookies 6
Aviso de cookies 6
Quais cookies utilizamos? 6
X. Segurança da informação 7
XI. Plano de Reposta a incidentes de Segurança 7
O que é um incidente de segurança? 7
Equipe de resposta e áreas de suporte 7
Investigação 7
Contenção, erradicação e recuperação 8
Comunicação à ANPD 9
i. Em que situação a ANPD deverá ser comunicada? 9
ii. Como comunicar um incidente e quais informações devem ser informadas à ANPD? 9
iii. Em quanto tempo a ANPD deverá ser comunicada? 10
Comunicação ao titular de dados e aos parceiros 10
Relatório do incidente de segurança 10
XII. Treinamentos 11
XIII. Penalidades 11

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

I. Apresentação

Este Manual, juntamente com a Política de Privacidade e Proteção de Dados (Política) e demais regramentos eventualmente elaborados, faz parte do Programa de Governança em Privacidade e Proteção de Dados (PGPD) da Ventura Petróleo S/A (Ventura ou Empresa) e é de observância obrigatória por todos os seus colaboradores, Conselheiros, membros de Comitês, membros da Diretoria Executiva, empregados, estagiários, sócios, parceiros e terceiros.

O PGPD busca fornecer aos integrantes da Ventura elementos suficientes para o uso e tratamento de dados pessoais e documentos, de modo a garantir aos clientes e titulares de dados a devida segurança e o sigilo nos limites estabelecidos pela Lei Geral de Proteção de Dados (LGPD).

Em conjunto com a Política, o Manual objetiva consolidar orientações e regulamentar procedimentos necessários à aplicação de mecanismos internos de segurança da informação, garantindo o sigilo profissional, legal e empresarial, e colocando em prática os princípios e encargos impostos pela LGPD. Também contém o regramento das políticas de incidentes de segurança e de utilização de cookies. O Manual é, portanto, um guia para conformidade com a LGPD e para a efetiva preservação de sigilo. A política de segurança da informação, que também é de observância obrigatória, e o guia de boas práticas são documentos separados, que integram o PGPD.

É natural existirem dúvidas ou casos omissos, os quais deverão ser encaminhados, em um primeiro momento, ao Encarregado, Portnet Tecnologia, nas pessoas do André Vieira e Gustavo Guimarães, que poderá ser contatado pessoalmente ou pelo e-mail encarregado@ventura-offshore.com. Entretanto, sempre que as mencionadas dúvidas ou omissões envolverem dados de pessoas não integrantes da Empresa, o Comitê de Conformidade poderá ser consultado.

II. Aplicabilidade da LGPD

Do que a lei trata?

A LGPD dispõe sobre o tratamento de dados pessoais, como p. ex. nome, número de identidade, etnia, crença religiosa, inclusive nos meios digitais, por pessoa física (que exerça atividade econômica) ou por pessoa jurídica de direito público ou privado. Seu principal objetivo é a proteção dos direitos fundamentais de liberdade e de privacidade.

Nos termos da lei, tratamento é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou ao controle da informação, modificação, comunicação, transferência, difusão ou extração.

Quando a LGPD é aplicável?

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, desde que ocorra uma das seguintes hipóteses:

- o tratamento tenha sido realizado no território nacional;
- o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- os dados pessoais tenham sido coletados no território nacional (o titular encontrava-se no território nacional no momento da coleta).

As hipóteses são amplas e, no âmbito de uma empresa privada, podem afetar todos os setores.

O tratamento inclui, por exemplo, a coleta e utilização de dados pessoais dos sócios, colaboradores de empresas contratadas, empregados, fornecedores ou clientes. No âmbito da Ventura é provável que a atuação em processos judiciais ou administrativos, bem como a celebração de contratos, contenha dados pessoais, o que atrai a incidência da Lei.

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY

III. Conceitos (da LGPD)

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: 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;

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

Agentes de tratamento: o controlador e o operador;

Tratamento: toda operação realizada com dados pessoais, como as que se referem à 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, 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: 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;

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY

IV. Princípios

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

V. Autorização de tratamento

Há diversas hipóteses legais, previstas no Artigo 7º da Lei, em que é permitido o tratamento de dados sem autorização específica, como p. ex., quando o tratamento for necessário para o cumprimento de obrigação legal ou regulatória; a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e/ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Em quaisquer dessas hipóteses, é dispensada a autorização do titular para o tratamento.

Solicitação de autorização de uso e compartilhamento dados

A Empresa, caso necessário, buscará obter autorização do titular para o tratamento de dados por meio de autorização específica.

Modo de solicitação por titulares de dados pessoais

O exercício de quaisquer direitos previstos no Artigo 18 da Lei pelo titular poderá ocorrer a qualquer momento, mediante requisição a ser feita por escrito para o endereço físico da Empresa ou para o e-mail encarregado@ventura-offshore.com ou via link do portal de privacidade presente no banner de cookies.

Este aviso deverá constar no site da Empresa.

Conforme a LGPD, o titular tem os seguintes direitos: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço

ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e IX - revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Modo de atendimento à solicitação de titulares de dados pessoais

Feita a requisição pelo titular, ela deverá, segundo a Lei, ser respondida em prazo razoável. Enquanto não houver regulamentação específica que determine o tempo máximo para resposta, a Empresa estabelece o prazo de 10 dias úteis, prorrogáveis por igual período, para responder as solicitações, desde que a prorrogação seja motivada e informada ao titular.

O Encarregado poderá requisitar auxílio de quaisquer equipes e de colaboradores para responder a requisição do titular. Eventual negativa de auxílio, formal ou não, poderá ser analisada pela área de Compliance e/ou Comitê de Conformidade, e poderá sujeitar a(s) equipe(s) e/ou colaborador(es) às sanções disciplinares previstas nos regramentos da Empresa e na legislação trabalhista.

O titular deverá receber, por escrito via portal de privacidade da plataforma da Privacy Tools, informações sobre o andamento do processo de resposta à sua requisição até que ela seja integralmente atendida ou negada.

VI. Fluxo de dados

Os fluxogramas anexados ao relatório de impacto estão divididos por setores, considerado o organograma da Empresa, e contêm informações sobre: **coleta, tratamento, transferência e compartilhamento, envio e recebimento internacionais, finalidade do tratamento, armazenamento de dados, e término do tratamento do tratamento de dados**.

Eles podem ser encontrados ao final do relatório de impacto, serão atualizados de tempos em tempos, conforme ocorrerem mudanças e melhorias no tratamento de dados de cada um dos setores da empresa, mas são de acesso restrito.

VII. Classificação de dados

Dados pessoais

Dados pessoal é qualquer tipo de informação relacionada a pessoa natural ou pessoa física.

Dados sensíveis

Dado sensível é qualquer dado da pessoa natural que de alguma forma esteja relacionado a 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, e dado genético ou biométrico.

Dados sigilosos

Dado sigiloso é aquele que se enquadra em alguma hipótese constitucional e/ou legal de sigilo ou segredo de justiça, como por exemplo dados protegidos pelo sigilo profissional, fiscal, bancário, telefônico e telemático dados pessoais em posse do poder público, dados que possam pôr em risco a segurança de seu titular, tais como algumas informações patrimoniais. São, ainda, consideradas sigilosas informações classificadas como imprescindíveis à segurança da sociedade e do Estado, nos termos da Lei de Acesso à Informação.

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY

VIII. Avaliação do risco – matriz risco

A Avaliação de Risco será feita por cada área da empresa, em conjunto com a área de Tecnologia da Informação (TI) conforme matriz de risco. Ela será de acesso restrito para cada uma das áreas, para o encarregado e para a área de Compliance. Ela poderá ser compartilhada com a área de TI, a qual poderá opinar sobre a classificação de risco, e obrigatoriamente será compartilhada com o Comitê de Conformidade.

IX. Cookies

Cookies são pequenos arquivos enviados por sites e salvos no computador do usuário, por meio do navegador utilizado pelo usuário para acesso.

Para melhorar a experiência do usuário e para permitir a identificação de algumas informações, por exemplo, de onde acessa e o que acessa em nosso site, utilizamos cookies rastreadores. Esses cookies também são usados para definir a língua preferencial em que nosso site será exibido.

Usamos cookies em ligação com a Google Analytics. Essa é uma ferramenta do Google utilizada, em geral, em conjunto com Google Ads e Google Search Console para monitorar, de forma anonimizada, o perfil de quem acessa nosso site, páginas mais acessadas, origem do acesso e outros dados.

Opção quanto aos cookies

Será dada a opção ao usuário de aceitar todos os cookies, rejeitá-los todos ou um a um. O usuário será alertado, ainda, que a ausência de manifestação quanto aos cookies implicará aceitação. Nessa hipótese, a barra de aviso de cookies ficará disponível, mas isso não impedirá a navegação nas páginas do site.

Aviso de cookies

Além das informações constantes na política de privacidade, ao acessar nosso site, o usuário deverá ser informado sobre cada um dos tipos de cookies que utilizamos e deverá ter a opção de escolher quais deles aceita. A depender da escolha feita pelo usuário, o site guardará a informação e não perguntará novamente a este usuário identificado de maneira anonimizada.

O aviso de cookies conterá a frase *"Usamos cookies e tecnologias semelhantes, entre outros motivos, para melhorar a sua experiência de navegação em nosso ambiente e para permitir a identificação de algumas informações. Você pode escolher quais cookies aceita ou rejeita. Ao aceitar, você concorda com tal monitoramento e com os termos da nossa Política de Privacidade, a qual pode ser acessada aqui."*

Quais cookies utilizamos?

No site, haverá opção para escolher quais dos seguintes cookies, definidos pela Google Analytics e por nós usados, o usuário aceita utilizar:

a) "_ga" – utilizado para rastrear e contar as visualizações do site;

b) "_gat_ua-140537673-1" – utilizado para armazenar e rastrear sessões;

c) "gid" – utilizado para rastrear e contar as visualizações do site;

d) "pll_language" – utilizado para identificar em qual idioma o site deverá ser apresentado, com base nas preferências anteriores do usuário.

COPY NÃO CONTROLADA / NON CONTROLLED COPY

X. Segurança da informação

A política de segurança da informação, bem como o guia de boas práticas de segurança da informação e tratamento de dados pessoais, integra o PGPD e devem ser observados por todos os colaboradores. Esses documentos contêm regras e sugestões sobre como aumentar a segurança dos dados, pessoais ou não, tratados pela Empresa e são partes fundamentais do programa de governança. Eles visam, aumentar não apenas a segurança da empresa, mas de cada um dos indivíduos que dela fazem parte ou que com ela fazem negócios. Nesses documentos podem ser encontradas informações sobre as medidas de tecnologia da informação que a Ventura adota para proteger os dados pessoais que trata, bem como as ações que seus colaboradores devem tomar para proteger dados pessoais.

A leitura desses documentos é obrigatória. Não seguir as regras impostas na política de segurança da informação ou tentar violá-las pode sujeitar o(s) autor(es) a sanções previstas em regramentos da empresa, bem como na legislação aplicável incluindo a legislação trabalhista e a penal.

XI. Plano de Reposta a incidentes de Segurança

O que é um incidente de segurança?

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais ou sigilosos.

O Programa de Governança em Privacidade e Proteção de Dados da Ventura, como um todo, visa a impedir a ocorrência de qualquer evento adverso relacionado à segurança das informações. Contudo, na eventualidade de seu acontecimento, devem ser seguidas as diretrizes previstas neste Capítulo.

Equipe de resposta e áreas de suporte

A Ventura definirá quem integrará a equipe de resposta a incidentes ou o colaborador responsável por lidar com potenciais incidentes junto ao Encarregado. Além disso, designará as áreas de suporte que atuarão na ocorrência de incidentes, como Produção, Tecnologia da Informação (TI) e Encarregado.

Em caso de evento adverso, confirmado ou sob suspeita, relacionado à violação de segurança de dados pessoais ou dados sigilosos, a primeira pessoa que suspeitar do ocorrido deverá comunicar ao Encarregado, o qual contactará membros das Equipes potencialmente afetadas ou relacionadas, a seu critério, para lhes informar sobre a ocorrência. A área de Compliance também deverá ser informada. Essa equipe avaliará a gravidade do incidente, potencial ou confirmado, e reportará ao Comitê de Conformidade o evento adverso.

Investigação

Quando da ocorrência de incidente de segurança, a Empresa conduzirá processo de investigação destinado a identificar, coletar e preservar evidências do incidente, bem como descobrir a causa. Fará, ainda, prova positiva da investigação realizada, indicando quais medidas foram adotadas a fim de eliminar ou minimizar o risco de sanções e indenizações.

O incidente pode ser constatado, dentre outras formas, por meio de: (i) denúncia por parte dos titulares de dados, (ii) emprego de ferramentas automatizadas que detectam vazamento de dados e/ou tentativas de invasão aos sistemas eletrônicos ou físicos da empresa; (iii) reporte por parte de operador ou; (iv) notificação por parte de terceiro.

O processo de investigação que leva à identificação e coleta de evidências sobre o ocorrido será conduzido de maneira segura, ética, transparente, eficiente e sigilosa, observando os limites legais.

Verificada possível ocorrência de incidente, a investigação interna será composta pelas seguintes etapas, se aplicáveis, e na ordem que a equipe de investigação escolher:

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY

- Depoimento de testemunhas;
- Inspeção em dispositivos corporativos: serão analisados, conforme a necessidade do caso, tanto os dispositivos corporativos utilizados por colaboradores dentro da organização, quanto aqueles utilizados fora dela;
- Relatório: será elaborado pelo a partir de conclusões fundamentadas, sem a realização de juízo de valor (veja abaixo).

Se o incidente apontar a possibilidade de ato ilícito, providências como reporte a autoridades e punição trabalhista poderão ser adotadas.

Contenção, erradicação e recuperação

Para cessar a causa do incidente de segurança, quando possível e/ou cabível, a Empresa adotará medidas de contenção de curto e longo prazo. As medidas de curto prazo serão respostas imediatas para evitar que o incidente cause ou continue a causar danos, ou reduzi-los. A contenção de longo prazo abrange o restabelecimento dos sistemas da Empresa à sua condição normal após a neutralização ou solução do fato gerador do incidente.

As medidas de contenção poderão compreender, dentre outras providências:

- Interrupção do funcionamento de sistema de dados atingido;
- Coleta de equipamentos danificados;
- Restrição e/ou suspensão de acessos aos sistemas da Empresa;

A depender da gravidade do incidente, a Empresa poderá requerer ordens judiciais para cessar ou auxiliar na apuração de medida ilícita. Ainda, a depender da gravidade e da natureza do incidente, será adotado processo de restauração dos sistemas afetados. Se necessário, possível e conveniente, os sistemas poderão ser atualizados e melhorados para evitar a ocorrência de novo incidente do mesmo tipo.

Após a verificação da integridade dos sistemas após o incidente, serão avaliadas eventuais perdas de dados e/ou sistemas. Para evitar maiores danos e garantir o pronto restabelecimento do fluxo normal de informações, a Empresa manterá cópias de segurança em sistema de nuvem ou em armazenamento seguro.

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

Comunicação à ANPD

i. Em que situação a ANPD deverá ser comunicada?

Em caso de incidente de segurança que possa, ainda que potencialmente, acarretar risco ou dano ao titular do dado afetado, deverá ser feita comunicação à Autoridade Nacional de Proteção de Dados (ANPD). Ressalte-se que a comunicação deverá ocorrer ainda que haja mera suspeita de incidente de segurança e que eventual avaliação dos danos decorrentes do incidente possa vir a ser considerada violação à LGPD.

A ANPD sugere, para aferição quanto à necessidade ou não de comunicação, que os seguintes questionamentos sejam realizados:

1. Ocorreu um incidente de segurança relacionado a dados pessoais?

   ☐ Sim – Próxima pergunta.

   ☐ Não – Não é necessário comunicar a ANPD se não houve incidente de segurança relacionado a dados pessoais.

2. Existe um risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados em razão do incidente de segurança?

   ☐ Sim – Comunique à ANPD e ao titular.

   ☐ Não – A comunicação à ANPD não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

ii. Como comunicar um incidente e quais informações devem ser informadas à ANPD?

A comunicação à ANPD deverá ser feita por meio do preenchimento de formulário e peticionamento eletrônico[1].

Nos termos do Artigo 48 da LGPD, o controlador (e, eventualmente, o operador) deve ser o responsável por realizar a comunicação à ANPD e ao titular do dado. Esta comunicação, que poderá ser complementada em momento posterior, deverá ocorrer em prazo a ser definido pela ANPD e deve mencionar, no mínimo, os seguintes pontos:

a. a descrição da natureza dos dados pessoais afetados;
b. as informações sobre os titulares envolvidos;
c. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
d. os riscos relacionados ao incidente;
e. os motivos da demora, no caso de a comunicação não ter sido imediata; e
f. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

[1] Para mais informações acerca do peticionamento, acesse o link: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico

iii. Em quanto tempo a ANPD deverá ser comunicada?

A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, § 1º), a ser definido pela ANPD. Embora não tenha havido regulamentação nesse sentido, a realização da comunicação demonstra transparência e boa-fé e poderá ser considerada em processo de fiscalização e eventual aplicação de sanção administrativa.

Enquanto pendente a regulamentação, recomenda-se que, após a ciência do evento adverso e se houver risco relevante, a ANPD seja comunicada com a maior brevidade possível, considerando-se, a título indicativo, o prazo de 2 (dois) dias úteis, contados da data do conhecimento do incidente. Esse prazo foi estabelecido como parâmetro na definição de comunicação já existente no Decreto nº 9.936/2019, em virtude da necessidade de gerenciamento dos incidentes de segurança com dados pessoais por parte da ANPD e das consequências danosas que podem ocorrer em razão do atraso nas ações de contenção ou mitigação.

Comunicação ao titular de dados e aos parceiros

Também os titulares de dados devem ser informados sobre a ocorrência de incidente de segurança.

A ANPD ainda não estabeleceu prazo para tal providência, nem casos em que a comunicação aos titulares de dados poderá ser dispensada. No entanto, a Empresa adota a política de que deverá informar, em até 5 (cinco) dias úteis, titulares cujos dados tenham sido indevidamente acessados por não integrantes da Empresa.

Relatório do incidente de segurança

Encerrada a fase de investigação e reporte ao titular e/ou ANPD, deverá ser elaborado relatório, resumido ou detalhado, o qual deverá conter obrigatoriamente:

- Descrição do incidente;
- A equipe de investigação formada;
- Identificação dos impactos gerados;
- As conclusões da investigação;
- As medidas de contenção adotadas;
- A ocorrência ou não de reporte do incidente (em caso positivo, o reporte deverá ser anexado ao relatório); e
- As medidas de melhoria e prevenção a serem adotadas, caso necessário.

O relatório deverá ser arquivado e enviado à área de Compliance para avaliação. Esta o remeterá ao Comitê de Conformidade e, a critério deste, o relatório poderá ser compartilhado, no todo, em parte ou com tarjas, com alguns ou todos os integrantes da Empresa. O documento é parte do Programa de Conformidade e deverá ser mencionado, se cabível e possível, em futuros treinamentos. Trata-se de oportunidade para aprender com erros, se houver, e para implementar modificações no Programa de Conformidade e nos regramentos e treinamentos a ele relacionados.

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

XII. Treinamentos

A Ventura deverá divulgar amplamente a Política de Proteção de Dados, inclusive em seu site, e este Manual para todos sujeitos a seus termos.

O Encarregado é responsável pelo desenvolvimento e pela implementação de programa de treinamento de conscientização sobre a LGPD e Segurança da Informação, o qual deverá ser elaborado considerando as necessidades de diferentes colaboradores da Empresa, de acordo com suas funções e cargos.

Após os treinamentos iniciais, o Encarregado deverá monitorar a implementação de treinamentos para novos colaboradores, de acordo com sua necessidade. As áreas de Compliance e de Auditoria Interna poderão, a seus respectivos critérios, monitorar implementação e treinamentos relacionados ao PGPD. De igual modo, poderão elaborar relatórios a serem submetidos ao Comitê de Conformidade.

O treinamento deverá ser ministrado a novos integrantes quando de seu ingresso e periodicamente aos demais integrantes.

XIII. Penalidades

A observância à cultura e aos procedimentos de proteção de dados pessoais e sigilosos por parte de todos os membros da Empresa, além de ser um dever legal e ético, evitará a imposição de penalidades pela ANPD e poderá atenuar a aplicação destas em caso de eventual descumprimento da Lei.

Quando da violação à LGPD, a ANPD aplicará as sanções previstas no artigo 52 da LGPD, as quais variam entre aplicação de advertências, com indicação de prazo para adoção de medidas corretivas, multas, ou, ainda, a proibição total ou parcial de atividades relacionadas ao tratamento de dados.

A aplicação de qualquer penalidade poderá impactar significativamente na atividade da Empresa tanto no aspecto financeiro, quanto no reputacional, além de potencialmente gerar repercussões cíveis.

Ressalta-se que a ANPD deverá considerar parâmetros como: gravidade e natureza das infrações e dos direitos afetados, existência de mecanismos internos para correção e proteção de dados; pronta adoção de medidas; boa-fé; extensão do dano; condição econômica do infrator; adoção de política de boas práticas e governança em proteção de dados; reincidência, proporcionalidade da sanção; cooperação do infrator e vantagem auferida ou pretendida pelo infrator.

CÓPIA NÃO CONTROLADA / UNCONTROLLED COPY