Manual de Adequação e Conformidade para Tratamento de Dados Pessoais

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

Versão 1.0

Rondonópolis-MT, 05 de Setembro de 2022

MANUAL DE ADEQUAÇÃO E CONFORMIDADE PARA O TRATAMENTO DE DADOS PESSOAIS

Lei Geral de Proteção de Dados Pessoais -– LGPD

PREFEITURA DE RONDONÓPOLIS-MT

JOSÉ CARLOS JUNQUEIRA DE ARAÚJO
PREFEITO MUNICIPAL

AYLON GONÇALO DE ARRUDA
VICE-PREFEITO

NEIVA TEREZINHA DE CÓL
SECRETARIA DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

KÉSIA ELAINE PAULA COSTA DE ALMEIDA MARQUES
ENCARREGADA GERAL DE PROTEÇÃO DE DADOS

COMITÊ GESTOR DE IMPLANTAÇÃO DA LGPD

KATHIA LUISI MONTEIRO ELIAS DIAS
PRESIDENTE

MEMBROS:
ANDRÉA MACHADO MOURA DE SOUZA
DANIEL CAYRES LIMA
ÉDER DE OLIVEIRA
FABIANO KEIJI TAGUCHI
GUILHERME HENRIQUE MACHADO CHAVES
LUANA DE PAULA PEREIRA DA SILVA
SANDRA MARIA DA SILVA MACEDO

INTRODUÇÃO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei Nacional nº 13.709, de 14 de agosto de 2018, estabeleceu as regras gerais para a proteção dos dados pessoais e da privacidade dos cidadãos, e foi regulamentada no Município de Rondonópolis pelo Decreto nº 10.789/2022.

A Encarregada Geral de Proteção de Dados foi nomeada através do Decreto nº 11.006, de 16 de Agosto de 2022. E o Comitê Gestor da LGPD, através do Decreto nº 10.939, de 07 de Julho de 2022. Por essas normas, os agentes e servidores públicos devem conhecer e adotar as boas práticas de proteção e privacidade decorrentes de sua atividade funcional, preservando os direitos e garantias dos cidadãos em estrita conformidade com a lei.

A adequação do Município de Rondonópolis em relação à LGPD requer uma transformação cultural que alcançará os níveis estratégico, tático e operacional da instituição e deverá considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução, além de promover ações de conscientização de todo o corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Este manual visa apresentar as hipóteses de tratamento de dados, como também constam perguntas que objetivam facilitar a identificação da hipótese mais apropriada. E ainda apresenta as especificidades para o tratamento de dados de crianças e adolescentes, as políticas: de segurança da informação e de privacidade, algumas sugestões de cláusulas contratuais, modelos de termos de uso. Além disso, destacam-se obrigações com as quais o controlador e/ou operador deverá se comprometer ao optar por cada hipótese e apresenta o modelo de Relatório de Impacto de Proteção de Dados Pessoais.

2 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD (LEI Nº 13.709/2018)

A Lei Geral de Proteção de Dados – LGPD, instituída pela Lei Nacional n. 13.709, de 14 de agosto de 2018, versa sobre o tratamento de dados pessoais. Como dado pessoal, considera-se toda informação relacionada a pessoa natural identificada ou identificável, disposto em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Nos termos da LGPD, o titular dos dados pessoais tem direito ao acesso facilitado às informações sobre o tratamento de seus dados próprios, a qualquer momento e mediante solicitação. Todas as informações ao titular, inclusive autorizações de uso de dados, deverão ser disponibilizadas de forma clara, adequada e ostensiva.

Deste modo, antes de iniciar o tratamento de dados pessoais, o servidor em atividade deve se certificar, previamente, que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados, toda vez que a Lei assim o exigir.

O Município de Rondonópolis têm permissão legal para realizar o tratamento de dados pessoais unicamente para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que as hipóteses de tratamento sejam informadas ao titular.

Em se tratando de Administração Pública, a Lei procura não abrir espaço para interpretações, sendo necessário conhecer as exceções para a análise da aplicabilidade no tratamento de dados pessoais em geral (art. 7º), bem como, a correspondente base legal para o tratamento de dados pessoais sensíveis (art. 11), conforme as hipóteses a seguir:

3 HIPÓTESES DE TRATAMENTO

Segundo o art. 7º da Lei nº 13.709/2018, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- ✓ Tratamento mediante consentimento do titular;
- ✓ Cumprimento de obrigação legal ou regulatória;
- ✓ Execução de políticas públicas;
- ✓ Realização de estudos e pesquisas;
- ✓ Execução de contrato ou de procedimentos preliminares relacionados a contrato;
- ✓ Exercício de direitos em processo judicial, administrativo ou arbitral;
- ✓ Proteção da vida ou da incolumidade física do titular ou de terceiro;
- ✓ Tutela da saúde do titular; t
- ✓ Atender interesses legítimos do controlador ou de terceiro;
- ✓ Proteção do crédito; e
- ✓ Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

3.1 Tratamento para a execução de políticas públicas

Essa hipótese é aplicável para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Trata-se de uma hipótese que dispensa o consentimento do titular e que deve ser realizada por controladores que sejam pessoas jurídicas de direito público.

O Controlador pode, no entanto, envolver operadores para a realização do tratamento de dados pessoais necessários à consecução de políticas públicas. Estes últimos podem ser pessoas jurídicas de direito privado.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O controlador é pessoa jurídica de direito público?

2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?

3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?

4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?

5. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?

6. Será indicado um encarregado para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão?

Conforme o Art. 5º, inciso VIII da Lei nº 13709/2018 o encarregado é 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

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Segundo o Art. 23 da LGPD, os órgãos e entidades públicas deverão realizar o tratamento de dados apenas para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Nesse contexto, não havendo uma delimitação inequívoca das atribuições legais que poderiam ser diretamente relacionadas à execução de políticas públicas, cabe aos órgãos e entidades analisar, no caso concreto, a possibilidade enquadrar o tratamento do dado na hipótese prevista no Art. 7º, inciso III, combinada com o disposto no Art. 23 da LGPD.

3.2 Tratamento para o cumprimento de obrigação legal ou regulatória

Essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Não se enquadram nessa hipótese as obrigações estabelecidas por contrato.

Para enquadramento nessa hipótese, deve-se avaliar:

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?

2. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.3 Tratamento para a execução de contrato ou de procedimentos preliminares relacionados a contrato

Essa hipótese é aplicável para o tratamento de dados necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. As hipóteses de tratamento de dados estarão previstas no contrato. O consentimento é fornecido no ato de formalização do termo ou decorrente do mesmo.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?

Essa pergunta deve ser respondida positivamente para que tal hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.4 Tratamento mediante consentimento do titular

Essa é uma hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. Trata-se de hipótese possível quando as demais do art. 7º forem descartadas.

Uma vez descartadas as demais hipóteses, o órgão/entidade deve avaliar:

1. Será viável a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade?

2. Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado?

3. O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento?

Observações:

a) É vedado o tratamento de dados pessoais mediante vício de consentimento.

b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.

d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

4. Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado?

5. No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal?

Ressalta-se que todas as questões acima, se aplicáveis, devem ser respondidas positivamente para que a hipótese de tratamento do dado por consentimento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.5 Tratamento para a realização de estudos e pesquisas

Essa hipótese é aplicável para o tratamento de dados para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Para enquadramento nesta hipótese, deve-se avaliar:

1. O controlador ou operador é órgão de pesquisa?

2. Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa?

3. Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados?

4. O órgão de pesquisa garante que não serão revelados dados pessoais em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada?

5. O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.6 Tratamento para o exercício de direitos em processo judicial, administrativo ou arbitral

Essa hipótese é aplicável para o tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?

2. O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.7 Tratamento para a proteção da vida ou da incolumidade física do titular ou de terceiro

Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?

2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.8 Tratamento para a tutela da saúde do titular

Essa hipótese é aplicável para o tratamento de dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária?

2. O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.9 Tratamento para atender interesses legítimos do controlador ou de terceiro

Essa hipótese é aplicável para o tratamento de dados quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Órgãos e entidades públicas não devem recorrer a essa hipótese se o tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados?

2. O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?

3. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

4. Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

3.10 Tratamento para proteção do crédito

Essa hipótese é aplicável para o tratamento de dados para proteção do crédito do titular.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular?

2. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

4 ESPECIFICIDADES PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

A LGPD traz regramento específico para o tratamento de dados pessoais sensíveis, que são definidos no art. 5º, inciso II como "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".

São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida.

O art. 11 da LGPD elenca as hipóteses em que o tratamento de dados pessoais sensíveis pode ser realizado. Novamente, a lei traz a possibilidade de tratamento mediante consentimento do titular, como regra, e enumera as hipóteses que dispensam o consentimento, por meio de rol extensivo.

O tratamento mediante consentimento exige que se registre a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento.

Já o tratamento de dados pessoais sensíveis sem o fornecimento de consentimento do titular somente pode ocorrer nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (resguardados os direitos do titular mencionados no art. 9º da Lei sobre o acesso facilitado às informações quanto ao tratamento dos seus dados. A exceção a este item é no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais).

Observa-se que os órgãos e entidades da administração pública poderão enquadrar se em diversas hipóteses de dispensa de consentimento para o tratamento de dados de pessoais sensíveis.

No entanto, cabe destacar que a lei determina o tratamento desse tipo de dado apenas em situações indispensáveis. Isso traz para o controlador o ônus da prova da alegada indispensabilidade.

Os órgãos e entidades públicas que realizarem o tratamento dos dados pessoais sensíveis deverão dar publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei.

Especificamente no que tange à realização de estudos em saúde pública, o art. 13 da Lei possibilita que os órgãos tenham acesso a bases de dados pessoais, inclusive os atributos sensíveis, que serão tratados exclusivamente dentro do referido órgão e estritamente para a finalidade de realização de estudos e pesquisas. Nessa hipótese, o órgão ou entidade deverá garantir que os dados sejam mantidos em ambiente controlado e seguro, e que, sempre que possível, sejam anonimizados ou pseudonimizados.

A LGPD traz ressalva expressa à divulgação de dados pessoais quando da publicação de resultados ou de qualquer excerto de estudo ou de pesquisa realizada.

5 ESPECIFICIDADES PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Assim como para o caso das informações pessoais sensíveis, a LGPD dedica também atenção especial ao tratamento de dados de crianças e adolescentes.

A lei determina, em seu art. 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, mediante consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Nessa hipótese, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para acesso às informações tratadas.

É também dever do controlador envidar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável pela criança, consideradas as tecnologias disponíveis. Esse é, portanto, o desafio na coleta de dados pessoais de crianças e adolescentes, pois o consentimento é exigido inclusive no caso de execução de políticas públicas, o que não ocorre com adultos.

A única hipótese que dispensa o consentimento mencionado acima ocorre quando a coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros.

Contudo, a hipótese de coleta de consentimento dos pais ou responsáveis não se confunde com situações nas quais o tratamento do dado é necessário para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

Caso os órgãos e entidades públicas desenvolvam jogos, aplicações de internet ou outras atividades semelhantes voltadas ao público infanto-juvenil, a coleta de dados pessoais dos jovens deverá restringir-se ao estritamente necessário à atividade proposta.

6 NORMA TÉCNICA LGPD

A Norma Técnica têm por finalidade orientar sobre as medidas, os procedimentos, as diretrizes e modelos de documentações específicas para guiar a adequação e proteção no tratamento de dados pessoais na Administração Direta do Município de Rondonópolis.

As orientações disponibilizadas nas Normas Técnicas terão como base a Lei nº 12.527/2011, Lei nº 13.709/2018 e Decreto nº 10.789/2022, visto que a Encarregada Geral de Proteção de Dados e o Comitê Gestor de Implantação da Proteção Geral de Dados – LGPD são responsáveis pela elaboração de Normas Técnicas que regulamentarão os procedimentos para a proteção e tratamento de dados pessoais.

O operador deverá realizar o tratamento segundo as instruções fornecidas pela Encarregada Geral de Proteção de Dados, que verificará a observância das próprias instruções e das normas sobre a matéria.

As Normas Técnicas elaboradas e publicadas no sítio eletrônico oficial do Município aplicam-se aos órgãos e entidades da Administração Direta do Município de Rondonópolis.

As Normas Técnicas constarão regras específicas para a realização do tratamento e proteção de dados, e seus procedimentos operacionais no Município de Rondonópolis.

Cada Norma Técnica publicada será identificada por número sequencial em relação à norma anterior, iniciando em um, acrescido do ano de publicação da norma. Ex.: Norma Técnica LGPD 001/2020; Norma Técnica LGPD 002/2021. E deverá ser publicada no Diário Oficial Eletrônico – DIORONDON-e - Atos do Município e revogará automaticamente a norma anterior, quando regulamentar o mesmo assunto.

7 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.1 Introdução

A presente Política de Segurança da Informação ("Política") foi elaborada pelo Município De Rondonópolis – Estado De Mato Grosso, pessoa de direito público, situada à Avenida Duque De Caxias nº 1.000, Vila Aurora, no Município de Rondonópolis, Estado do Mato Grosso, inscrita no CNPJ sob o nº 03.347.101/0001-21 ("Prefeitura" ou "Nós") a fim de proteger os dados sob controle da Prefeitura, bem como os ativos físicos e tecnológicos por onde eles passam ou estão armazenados.

O principal objetivo da segurança da informação é proteger os dados e não somente os ativos físicos e tecnológicos por onde eles passam ou estão armazenados. A partir dessa premissa, existe uma independência nos conceitos da informação em relação à tecnologia

7.2 Critérios Gerais

A Política deve ser conhecida e acatada por todos os servidores, bem como estagiários, terceiros e prestadores de serviços que utilizam os recursos de processamento da informação de propriedade da Prefeitura, sendo de responsabilidade de cada um o seu cumprimento.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos servidores, bem como estagiários, quando na utilização dos recursos de processamento da informação da Prefeitura ou em ferramentas de comunicação privada não homologadas quando utilizadas em suas atividades laborais, ficando os transgressores sujeitos às sanções previstas pela Lei laboral (Estatuto do servidor, CLT – Consolidação das Leis do Trabalho), Civil (Código Civil) e Criminal (Código Penal).

Os documentos, programas e/ou sistemas produzidos pelos servidores, bem como estagiários, terceiros e prestadores de serviços por intermédio dos recursos de processamento da informação da Prefeitura são de propriedades da Prefeitura.

As informações de propriedade da Prefeitura devem ser utilizadas apenas para os propósitos definidos no Contrato Individual de Trabalho ou Contrato de Prestação de Serviços. Os servidores bem como estagiários, terceiros e prestadores de serviços não podem em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

7.3 O Que Queremos Proteger e Quem são os Responsáveis

É obrigação de todos os usuários dos sistemas da Prefeitura proteger os ativos de tecnologia e informação da Prefeitura. Essas informações devem ser protegidas contra acesso não autorizado, roubo e destruição. Os ativos de tecnologia e informação da Prefeitura são constituídos pelos seguintes componentes:

- Hardware de computador, CPU, disco, e-mail, web, servidores de aplicativos, sistemas de PC, software de aplicativo, software de sistema etc.
- Software de sistema, incluindo: sistemas operacionais, sistemas de gerenciamento de banco de dados e software de backup e restauração, protocolos de comunicação e assim por diante.
- Software de aplicação: utilizado pelos diversos departamentos da Prefeitura. Isso inclui aplicativos de software personalizados e pacotes de software de prateleira.
- Hardware e software de rede de comunicações, incluindo: roteadores, tabelas de roteamento, hubs, modens, firewalls, softwares e ferramentas de gerenciamento de rede associados.

7.4 Política de Senha/PIN

Um número de identificação pessoal (PIN) é um código de segurança para verificar sua identidade. Semelhante a uma senha, seu PIN deve ser mantido em sigilo porque permite o acesso a serviços importantes, como transações financeiras. Os PINs podem ser usados para qualquer coisa digital e que requeira acesso. Isso pode incluir dispositivos de comunicação, bloqueios de carro, bloqueios de casa e muito mais.

A segurança sempre será uma preocupação. Usar um PIN seguro é crucial para prevenir o acesso não autorizado às suas informações, contas e ativos.

Em hipótese alguma o PIN do usuário deverá ser escrito ou divulgado a servidores, terceiros, mídias sociais e qualquer outra forma inclusive à servidores do TI.

Após a identificação do usuário usando seu PIN pessoal na rede ou nos sistemas da Prefeitura, a responsabilidade por toda e qualquer atividade será única e exclusiva do usuário.

É proibida a divulgação do PIN e este não pode ser utilizado por terceiros em nenhuma circunstância.

Quaisquer ações indevidas efetuadas através do acesso autenticado serão de total responsabilidade do usuário identificado, ainda que seja durante eventual uso de seu PIN por terceiros, sujeitando o usuário às penalidades cabíveis.

7.5 Segurança de PIN

Como os PINs protegem muitas das suas informações e recursos, é aconselhável usar um PIN que seja difícil de adivinhar. Evite incluir os seguintes itens em seu PIN:

- Sequências de números simples como 1234 ou 0000
- Sequências de números repetidos como 1122 ou 2233
- Datas importantes, como seu ano de nascimento ou aniversário do cônjuge
- Qualquer parte do seu número de Seguro Social
- Qualquer parte do seu endereço ou número de telefone

PINs mais longos são mais seguros do que PINs mais curtos. Se você usar um PIN de quatro dígitos, há 10.000 variações possíveis (começando com 0000, 0001, 0002 e assim por diante). Com um PIN de seis dígitos, existem 1 milhão de códigos possíveis.

PINs mais longos funcionam bem porque são necessárias mais tentativas para adivinhá-los. A maioria dos sistemas de segurança bloqueia sua conta após um determinado número de tentativas. Isso garante que seja mais difícil para ladrões e programas de computador adivinharem o seu PIN.

7.6 Métodos para criar PINs seguros

Criar um PIN memorável pode ser difícil. Usar uma estratégia de PIN pode facilitar a criação de uma que você consiga lembrar.

Estratégia # 1: O Método da Palavra

Uma maneira de criar e lembrar um PIN é criá-lo a partir de uma palavra. Pense nos números e letras do teclado de um telefone. Você já usou a opção "discar por nome" para encontrar alguém na lista telefônica de uma empresa? Usando o mesmo conceito, você pode basear seu PIN em uma palavra, tornando-o mais fácil de lembrar.

Por exemplo, a palavra "WORD" é convertida no PIN 9673. O W está no 9, o O está no 6 e assim por diante.

Estratégia # 2: o método de data aleatória

Outra maneira de criar e lembrar um bom PIN é usar uma data não relacionada a você de forma alguma.

Estratégia # 3: o método de contato por telefone celular falso

Seu celular provavelmente possui dezenas ou centenas de contatos. Adicione um novo contato falso e oculte seu PIN no número de telefone desse contato. Por exemplo, se o seu PIN for 3282, você pode adicionar o número de telefone 555-923-3282, exceto usar um número de telefone de aparência local - não um com o código de área 555 fictício. Isso faz uso do conceito de "esconder-se à vista de todos".

7.7 Uso da Internet/Web

Existem vários hábitos que você deve desenvolver para melhorar a segurança de suas atividades online. Embora a lista a seguir possa parecer muito para gerenciar, a maioria dessas recomendações é simples e segui-las aumentará significativamente a segurança de sua navegação:

Mantenha o software do navegador atualizado: isso é crucial, pois novos patches são frequentemente lançados para corrigir vulnerabilidades existentes no software do navegador. Esta recomendação não se aplica apenas ao software do navegador - é fundamental manter o software do sistema operacional e qualquer outro software atualizado pelo mesmo motivo.

Execute o software antivírus: o software antivírus fornece proteção ao verificar e remover arquivos maliciosos do computador. Existem muitas opções excelentes de software de proteção contra vírus (pagos e gratuitos), portanto, cabe a você fazer uma pequena pesquisa e selecionar o programa que melhor se adapta às suas necessidades.

Verifique os arquivos antes de fazer o download: é importante evitar fazer download de nada até ter certeza de que é seguro. Se você tiver alguma suspeita de que um

arquivo pode não ser legítimo ou estar infectado, verifique-o com um software antivírus antes de fazer o download.

Cuidado com o phishing: os ataques de phishing usam comunicações online (geralmente e- mail) para induzir os usuários a fornecer suas informações confidenciais. Muitas vezes, essas mensagens parecem ser de bancos, sites de mídia social, sites de compras ou processadores de pagamento. As mensagens de phishing frequentemente contêm links que levam a versões falsificadas de sites populares. Você pode evitar ser vítima de esquemas de phishing, ignorando mensagens não solicitadas e não clicando em hiperlinks ou anexos em e-mails (digite ou copie / cole o URL como ele aparece).

Não reutilize senhas: usar a mesma senha para vários sites torna mais fácil para os invasores comprometerem suas informações confidenciais. Em vez disso, controle suas diferentes senhas com uma lista manuscrita que você mantém em um lugar seguro ou crie seu próprio algoritmo para criar senhas exclusivas que só você saberá. Também é recomendável que você altere suas senhas a cada 90 dias.

Use HTTPS: O "s" em "https" significa seguro, o que significa que o site está usando criptografia SSL. Verifique se há um "https:" ou um ícone de cadeado na barra de URL do seu navegador para verificar se um site é seguro antes de inserir qualquer informação pessoal.

Leia as políticas de privacidade: as políticas de privacidade e acordos do usuário dos sites devem fornecer detalhes sobre como suas informações estão sendo coletadas e protegidas, bem como como esse site rastreia sua atividade online. Sites que não fornecem essas informações em suas políticas geralmente devem ser evitados.

Monitore regularmente seus extratos bancários: ficar de olho em seus extratos on-line permitirá que você reaja rapidamente no caso de sua conta ser comprometida.

Evite Wi-Fi público ou gratuito: os invasores costumam usar farejadores sem fio para roubar informações dos usuários à medida que são enviadas por redes desprotegidas. A melhor maneira de se proteger disso é evitar o uso dessas redes por completo.

Desative as senhas armazenadas: Quase todos os navegadores e muitos sites em geral oferecem para lembrar suas senhas para uso futuro. Habilitar esse recurso armazena suas senhas em um local no computador, tornando mais fácil para um invasor descobrir se o sistema foi comprometido. Se você tiver esse recurso ativado, desative-o e apague suas senhas armazenadas.

Ative o bloqueador de pop-ups do seu navegador: o bloqueio de pop-ups agora é um recurso padrão do navegador e deve ser ativado sempre que você estiver navegando na web.

Se for necessário desativá-lo para um programa específico, ative-o novamente assim que a atividade for concluída.

7.8 Controles de Dispositivo

Os servidores estão mais familiarizados com seus próprios pertences, então não há virtualmente nenhuma curva de aprendizado quando eles vão para a mobilidade. Sua produtividade pode aumentar. Podem otimizar o tempo entre atividades pessoais e corporativas. Podem complementar seu acesso a tecnologias emergentes, mantendo-se atualizados com as últimas tendências.

Equipamentos cobertos por esta política:

- Desktops, laptops e tablets;
- Smartphones (definido como qualquer telefone celular que se conecta à Internet via Wi- Fi ou rede de operadora de celular);
- Flash, memória e / ou pen drives;
- Discos rígidos externos;
- iPods, iTouches e dispositivos de entretenimento e música portáteis semelhantes que se conectam a redes WiFi;
- Consoles de entretenimento e jogos que se conectam a redes Wi-Fi e são usados para acessar e-mail e sistemas da organização;
- Dispositivos vestíveis, como relógios, fones de ouvido de RV e óculos de realidade aumentada com WiFi ou Bluetooth.

Servidores que façam uso de notebooks, laptops, IPADs, Smartphones e outros dispositivos móveis contendo informações da Prefeitura, devem zelar pela segurança física do equipamento.

Tais dispositivos não devem ser expostos em locais públicos e devem-se tomar cuidados especiais para evitar-se perda ou roubo destes.

Dados em mídia removível, como por exemplo, DVDs, CD-ROM, pen drives e outros, quando não utilizados, devem estar armazenados em locais seguros, como por exemplo, cofres, gavetas com chave e outros.

7.9 Correio Eletrônico

Fica proibido o uso do correio eletrônico corporativo para cadastramento em sites do tipo: Compras Coletivas (Grupon, Clickon, Peixe Urbano etc.), Recrutamento e Seleção (Linkedin, Catho, Vagas etc.), Redes Sociais (Facebook, Instagram, Tik Tok, Youtube, etc.), Comércio Eletrônico (Mercado Livre, Lojas Americanas etc.) entre outros.

Estão terminantemente proibidas mensagens eletrônicas que possuam conteúdo ofensivo, preconceituoso ou discriminatório de qualquer natureza, como por exemplo, raça, sexo, religião, pornográfico ou obsceno, piadas, correntes, venda de produtos, caridade e outros.

Também fica proibida a utilização de aplicativos de mensagens instantâneas (Whatasapp, Telegram, etc.) e/ou redes sociais (Facebook, Instagram, etc.) para a realização de comunicações referentes aos dados e ativos da Prefeitura, seus clientes e fornecedores, seja para comunicação interna ou externa. Para a realização de comunicações internas ou externas devem ser utilizados os meios de comunicação oficiais e outorgados pela Prefeitura.

Todas as mensagens eletrônicas enviadas ou recebidas e/ou armazenadas nos computadores são de propriedade da Prefeitura.

Não é permitido o envio de cópias de mensagens eletrônicas internas contendo informações sensíveis ou confidenciais da Prefeitura para endereços externos sem a prévia autorização da Secretaria responsável.

Não é permitida a leitura ou o envio de mensagens eletrônicas, utilizando a caixa postal de outro usuário. Em caso de férias ou afastamento é necessário que as mensagens recebidas neste período sejam direcionadas para o servidor que assumirá suas funções no respectivo período.

É proibido o recebimento de arquivos pessoais advindos de fontes externas e não relacionadas a Prefeitura. Tais arquivos podem conter vírus ou programas com conteúdo não aprovado pela Prefeitura.

Mensalmente, cada usuário deverá excluir de sua caixa postal (Caixa de Entrada e Mensagens Enviadas) as mensagens que não sejam mais necessárias às suas atividades profissionais, preferencialmente aquelas que contenham informação sensível ou confidencial. Com isso, ajuda-se a manter a segurança e evita-se o uso desnecessário dos recursos computacionais da Prefeitura.

7.10 Utilização dos Arquivos

Todos os arquivos críticos ou vitais para a operação da Prefeitura devem estar armazenados nos servidores de arquivos designados.

A definição dos arquivos críticos é de responsabilidade da Secretaria responsável. Desta forma, são garantidas a segurança e a proteção destas informações contra roubo, perda e indisponibilidade.

Os arquivos devem ser identificados corretamente na rede, tendo seu nome relacionado com seu conteúdo. Deve-se evitar o uso de nomes comuns (e.g., Prefeitura, procedimentos, relatório) que podem facilmente criar duplicidade na rede e dificuldade de identificação dos mesmos.

Os arquivos são armazenados através de estrutura departamental em diretórios restritos a cada Secretaria. Não é permitido o acesso a arquivos de outras Secretaria, a menos que estes estejam no diretório público da Prefeitura.

Arquivos que deixem de ter importância para Prefeitura devem ser removidos do sistema. Esta limpeza é de responsabilidade de cada usuário e deve ser realizada frequentemente.

7.11 Disponibilização de Informações

Todos os comunicados internos formais emitidos a grupos de servidores através de mensagens eletrônicas ou impressos em murais ou quadro de avisos da Prefeitura devem conter: data e ano do término do comunicado; nome, cargo, unidade e área de atuação do responsável pelas informações divulgadas.

É proibido fornecer dados ou alterações de configurações solicitadas por telefone ou qualquer outro meio de comunicação.

Ao convocar reuniões, envolver somente as pessoas que efetivamente estejam relacionadas ao assunto abordado ou que necessitem ter acesso a tais informações pela natureza da posição que ocupam.

Para a realização de reuniões, internas ou externas, deve-se restringir o número de cópias dos documentos ao número de participantes.

Documentos contendo informações sigilosas ou importantes da Prefeitura não podem ser deixados sobre as mesas de trabalho ou de reunião ao alcance de quaisquer outras pessoas. Devem ficar à mostra apenas durante o seu uso e ao final devem ser novamente guardados em armários trancados, quando não mais estiverem sendo utilizados. A prática da mesa limpa deve ser sempre verificada pelo gestor da Secretaria.

O mesmo deve acontecer para informações escritas em quadros-brancos ou em flip-charts durante reuniões. Os servidores da Prefeitura devem preocupar-se em recolher as folhas do flip-chart e apagar o quadro-branco após o uso.

Recomenda-se que, dentro do possível, os servidores evitem o armazenamento de informações de trabalho em documentos físicos, de modo que a impressão de documentos apenas deverá ser realizada quando estritamente necessário.

Não havendo obrigação legal ou regulatória de armazenamento e guarda dos documentos, recomenda-se a eliminação imediata, utilizando-se fragmentadora de papeis, após a sua utilização.

O servidor deve evitar conversas sobre informações confidenciais da Prefeitura, como por exemplo, lançamentos, movimentos organizacionais, iniciativas, projetos e outros em locais públicos, táxis, bares, restaurantes, etc. Pessoas mal-intencionadas podem escutar tais informações e usá-las de maneira incorreta, visando prejudicar a Prefeitura.

7.12 Responsabilidades do usuário

O usuário não deve tentar alterar ou desativar nenhuma configuração de segurança aplicada ao dispositivo pelo departamento de TI.

O usuário deve consultar o fabricante / fornecedor / operadora para obter suporte de seu dispositivo antes de solicitar assistência do departamento de TI.

O usuário deve utilizar de forma idônea sua(s) conta(s) de identificação na rede e nos sistemas de computadores.

O usuário deve manter o sigilo e não fazer o uso privado de informações geradas, adquiridas ou utilizadas pela Prefeitura, às quais tenha tido acesso no exercício de suas atividades.

O usuário deve manter o sigilo de suas senhas de acesso aos recursos, sistemas e serviços da rede de computadores.

O usuário deve manter segura as informações manuseadas no âmbito da rede de computadores da Prefeitura.

O usuário deve observar que as informações armazenadas na estação de trabalho e nos demais dispositivos móveis utilizados para o desempenho de suas funções serão de sua inteira responsabilidade, não havendo previsão de backup para tais unidades.

O usuário deve manter a guarda, a segurança e a integridade dos ativos físicos e lógicos que estejam sob sua responsabilidade.

O usuário deve responder por todos os atos efetivados por meio de seu identificador, tais como login de rede e endereço de correio eletrônico.

O usuário deve utilizar os sistemas e serviços de informação somente para fins legais.

O usuário deve manter o sigilo de informações sensíveis para Prefeitura, sob qualquer circunstância de terceiros que não tenham a devida autorização de acesso a estas.

Ao compartilhar assuntos de trabalho, em qualquer local, dentro ou fora do ambiente de trabalho, a partir de qualquer tipo de canal, mídia, ferramenta ou tecnologia, o servidor deve respeitar a ética, a legislação vigente no Brasil e cumprir com seu dever de sigilo profissional.

No caso de um usuário acreditar que um dispositivo de propriedade ou fornecido pessoalmente que está autorizado a se conectar aos recursos, sistemas ou redes da organização pode estar infectado com um vírus, infecção por spyware ou outra ameaça de malware ou pode estar de alguma forma comprometido, ele deve notificar imediatamente o departamento de TI por escrito sobre o risco potencial à segurança.

Se um usuário perder ou perder um dispositivo de propriedade pessoal ou fornecido pessoalmente que está autorizado a se conectar aos recursos, sistemas ou redes da organização, ele deve notificar imediatamente o departamento de TI por escrito sobre o risco potencial de segurança.

Sempre que um usuário desativa, se prepara para retornar ou de outra forma deixa de usar um dispositivo de propriedade pessoal ou fornecido pessoalmente que o diretor de TI autorizou para uso da organização, o usuário deve notificar o departamento de TI de que o dispositivo não será mais usado para se conectar aos recursos da organização, sistemas ou redes.

Os usuários não podem descartar dispositivos previamente autorizados até que o departamento de TI aprove o dispositivo para descarte.

É vedado ao usuário emitir opiniões anônimas na Internet e na Intranet (mídias sociais, correio eletrônico, bate-papo, entre outros).

É vedado ao usuário utilizar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material que viole a lei de direitos autorais – Lei 9.610 de 19 de fevereiro de 1998;

É vedado ao usuário tomar ação própria no intuito de conter um incidente de segurança dos ativos de TI sob qualquer circunstância.

É vedado ao usuário promover atividades comerciais próprias ou de terceiros, incluindo oferta de serviços ou produtos, salvo por meio de canais institucionais adequados.

É vedado ao usuário enviar mensagens não institucionais para grupos ou pessoas que não as solicitaram ou autorizaram.

É vedado ao usuário enviar mensagens cuja veracidade não possa ser confirmada.

É vedado ao usuário enviar mensagens que, de alguma forma, violem as legislações vigentes.

É vedado ao usuário enviar mensagens, imagens, vídeos ou áudios ofensivos, depreciativos ou que impliquem em humilhação ou assédio, para outros servidores ou em grupos de compartilhamento criados para tratar de assuntos laborais em ferramentas de comunicação privada não homologadas pela Prefeitura.

7.13. Revisão da Política

Esta Política pode ser atualizada de tempos em tempos pela Prefeitura para refletir qualquer mudança na legislação ou nos métodos e práticas da Prefeitura.

7.14. Aplicação da Política

A violação de qualquer um dos princípios dentro da Política pode resultar em um processo administrativo (no caso de servidores) ou uma grave quebra contratual (no caso de terceiros), podendo equivaler a uma transgressão grave, o que poderá resultar em exoneração com justa causa ou rescisão contratual.

Esta Política não se destina e não concede aos usuários quaisquer direitos contratuais.

8 POLÍTICA DE PRIVACIDADE DOS SERVIDORES PÚBLICOS

8.1 Introdução

Como seu contratante, o Município De Rondonópolis – Estado De Mato Grosso, pessoa de direito público, situada à Avenida Duque De Caxias nº 1.000, Vila Aurora, no Município De Rondonópolis, Estado do Mato Grosso, inscrita no CNPJ sob o nº 03.347.101/0001-21 ("Prefeitura" ou "Nós") coleta e armazena seus dados pessoais. Nós utilizamos seus dados para fins de administração do corpo de servidores. Isso inclui, sem limitação, pagamento do salário e acesso ao holerite, acesso ao e-mail corporativo, gestão do corpo de servidores, cumprimentos de obrigações legais e regulatórias, bem como as demais finalidades necessárias para cumprimento de seus direitos e deveres como servidor público.

8.2 Objetivo

A presente Política de Privacidade dos Servidores Públicos ("Política") visa esclarecer como a Prefeitura realiza o tratamento de seus dados pessoais em situações específicas, indicando a finalidade do tratamento, possíveis transferências de dados pessoais a terceiros, o tempo de armazenamento dos dados coletados, bem como seus direitos como titular dos dados pessoais.

Todos os termos utilizados na redação desta Política terão os significados que lhes são outorgados na LGPD.

Em caso de dúvidas relacionadas ao conteúdo da presente Política, entre em contato conosco através do e-mail: dpo_enc.geral@rondonopolis.mt.gov.,br e/ou telefone nº (66) 98412-7310.

Estamos à disposição para ajudá-lo e mantê-lo informado sempre.

8.3 Dados Pessoais Coletados

A Prefeitura coleta, processa e armazena seus dados pessoais. Os dados pessoais incluem, mas não se limitam a:

Holerite

- CPF
- E-mail
- Senha

E-mail corporativo

• Nome de Usuário

• Senha

Notificação de Acidente de Trabalho – COVID-19

- Nome
- Nome da Mãe
- Sexo
- Data de Nascimento
- Estado Civil
- Telefone
- RG
- CPF
- Endereço
- Matrícula
- Cargo e Secretaria
- Data do afastamento e primeiros sintomas
- Dados do local de trabalho
- Atestado/Relatório Médico
- Exame Laboratorial Positivo para COVID-19
- Folha Ponto
- Assinatura

Notificação de Acidente de Trabalho – NAT

- Nome
- Nome da Mãe
- Sexo
- Data de Nascimento
- Estado Civil
- Telefone
- RG
- CPF

- Endereço
- Matrícula
- Cargo e Secretaria
- Data e hora do acidente
- Local do acidente
- Detalhes do acidente
- Endereço do acidente
- Dados das testemunhas que presenciaram o acidente (nome, endereço, telefone)
- Assinatura
- Relatório/Atestado Médico
- Boletim de Ocorrência
- Folha ponto
- Formulário do Sistema de Informação de Agravo de Notificação – SINAN.

Requerimento de Perícia Médica - RPM

- Nome
- Matrícula
- RG
- CPF
- Cargo
- Secretaria
- Endereço
- Telefone
- Motivo do Requerimento
- Nome da pessoa enferma e relação de parentesco
- Assinatura

Requerimento de Prorrogação de Licença Maternidade

- Nome
- Matrícula
- Cargo
- Assinatura

Requerimento de Adicional de Insalubridade/Periculosidade

- Nome
- Matrícula
- RG
- CPF
- Cargo
- Secretaria
- Telefone
- Motivo do Requerimento
- Justificativa para o Requerimento
- Assinatura

Requerimento de Redução da Carga Horária para Atender Pessoa com Deficiência

- Nome
- Sexo
- Matrícula
- Data de Nascimento
- Idade
- Telefone
- RG
- CPF
- Endereço
- Cargo
- Identificação da Pessoa com Deficiência (Nome, Sexo, RG, CPF, Data de Nascimento, Idade, Grau de Parentesco)
- Motivo do requerimento
- Certidão de Nascimento da Pessoa com Deficiência
- Certidão de Casamento ou equivalente
- Termo de Guarda, Tutela, Curatela ou Interdição para o servidor que, por determinação judicial, tenha sob sua responsabilidade pessoa com deficiência
- Escritura pública lavrada em cartório declarando a dependência econômica e social da pessoa com deficiência
- Laudo médico

- Exames complementares

Requerimento de Perfil Profissiográfico Previdenciário - PPP

- Nome
- Matrícula
- Data de Nascimento
- Idade
- RG
- CPF
- Endereço
- Telefone
- Cargo
- Assinatura
- Comprovante de endereço
- Certidão de casamento
- PIS/PASEP
- CTPS.

ServSaúde

- CPF

Suporte

- Usuário
- Senha

Sigeduca

- Usuário
- Senha
- E-mail

8.4 Finalidade do Tratamento de Dados Pessoais

Os dados pessoais que coletamos de você podem vir a ser utilizados para qualquer uma das seguintes finalidades:

Holerite

• Garantia de acesso ao sistema interno da Prefeitura para consulta e acesso ao holerite.

E-mail corporativo

• Acesso ao e-mail corporativo da Prefeitura para realização das atividades do dia a dia de trabalho.

Notificação de Acidente de Trabalho – COVID-19

• Comunicação para a Prefeitura acerca da contaminação do servidor público com COVID-19, para fins de afastamento temporário do servidor.

Notificação de Acidente de Trabalho – NAT

• Comunicação para a Prefeitura acerca de acidente de trabalho envolvendo servidor público, para fins de afastamento temporário do servidor.

Requerimento de Perícia Médica - RPM

• Comunicação para a Prefeitura acerca de requerimento de licença para tratamento de saúde.

Requerimento de Prorrogação de Licença Maternidade

• Comunicação para a Prefeitura acerca de requerimento de prorrogação de licença maternidade.

Requerimento de Adicional de Insalubridade/Periculosidade

• Comunicação para a Prefeitura acerca de requerimento de adicional de insalubridade/periculosidade.

Requerimento de Redução da Carga Horária para Atender Pessoa com Deficiência

• Comunicação para a Prefeitura acerca de requerimento para redução da carga horária de trabalho do servidor para atender pessoa com deficiência, nos termos da Lei nº 8.563/2015.

Requerimento de Perfil Profissiográfico Previdenciário - PPP

• Comunicação para a Prefeitura acerca de requerimento para elaboração do PERFIL PROFISSIOGRÁFICO PREVIDENCIÁRIO – PPP previsto na Constituição Federal artigo 40, § 4º, inciso III, Lei 8.213/91, Súmula Vinculante 33 e Instrução Normativa MPS/SPPS Nº 03/2014.

ServSaúde

• Garantia de acesso do servidor ao sistema ServSaúde.

Suporte

• Serviços de suporte de informática para o servidor público.

Sigeduca

• Acesso ao sistema Sigeduca.

Outras Finalidades

• Cumprimento de obrigações legais e regulatórias;

• Execução de políticas públicas;

• Exercício de outras atividades essenciais para a regular operação da Prefeitura, no âmbito de seu objeto social.

• Para prestar serviços relacionados ao trabalho: Tratamos seus dados pessoais para serviços financeiros, contábeis, folha de pagamento e compensação, recompensas e benefícios de reembolso, sucessão e planejamento de recursos em relação aos serviços relacionados ao trabalho.

• Para enviar e-mails periódicos: O endereço de e-mail que você fornece será usado para enviar informações e atualizações relativas ao trabalho dentro da Prefeitura.

• Obter serviços de terceiros: Também compartilhamos dados pessoais e outras informações com terceiros que prestam serviços para Prefeitura, tais como gerenciamento de sites, tecnologia da informação e fornecimento de infraestrutura relacionada, atendimento ao cliente, entrega de e-mail, auditoria e outros serviços semelhantes. Quando a Prefeitura compartilha dados pessoais com terceiros prestadores de serviços, exigimos que eles usem seus

dados pessoais apenas para a prestação de serviços para nós e sujeitos a termos consistentes com esta Política.

8.5 Compartilhamento de Dados Pessoais

A Prefeitura não compartilha, vende, aluga ou negocia suas informações pessoais coletadas com terceiros para fins promocionais ou conforme descrito neste Política.

A Prefeitura pode compartilhar dados pessoais com prestadores de serviços terceirizados contratados para fornecer serviços relacionados ao trabalho, benefícios e outros fins comerciais. Esses provedores de serviços terceirizados só podem usar os dados pessoais que fornecemos a eles conforme solicitado e instruído por nós. Além disso, a Prefeitura pode divulgar seus dados pessoais para cumprir obrigações legais ou regulatórias, exercício regular de direitos, responder a solicitações de autoridades governamentais ou auxiliar na prevenção e detecção de fraudes.

Ao conduzir negócios, trabalhar em projetos da Prefeitura ou implementar novos processos ou sistemas, uma operação pode exigir a transferência de informações pessoais para outras entidades públicas, sendo certo que a Prefeitura utiliza os remédios legais necessários para garantir a segurança, privacidade e proteção de seus dados pessoais.

8.6 Segurança dos Dados Pessoais

Seus dados pessoais são acessíveis apenas por aqueles servidores da Prefeitura que estão em sua Secretaria de recursos humanos ou que são secretários de operações e aqueles que precisam ter acesso ao banco de dados para o devido desempenho de suas funções. Existem medidas de segurança que garantem que o acesso seja negado a todos os outros servidores da Prefeitura e por terceiros.

8.7 Retenção e Descarte de Dados Pessoais

Os dados pessoais serão retidos apenas enquanto necessário para o cumprimento dos propósitos acima indicados, e deverão ser descartadas posteriormente. Reteremos suas informações enquanto você permanecer na qualidade de servidor da Prefeitura e reteremos suas informações por um período adicional de 30 (trinta) anos após sua saída da Prefeitura para fins

de cumprimento com obrigações legais e regulatórias. Caso, após sua saída da Prefeitura, você deseje solicitar uma revisão dos dados pessoais armazenados, bem como a eventual possibilidade de eliminação/anonimização daqueles dados passíveis de esquecimento, entre em contato conosco. Responderemos ao seu pedido para acessar ou excluir suas informações dentro de 15 (quinze) dias. Reteremos e usaremos suas informações conforme necessário para cumprir nossas obrigações legais, resolver disputas e fazer cumprir nossos acordos.

8.8 Controle dos Dados Pessoais

A Prefeitura também fornece aos titulares o direito de controlar seus dados pessoais, o que inclui o direito de acessar, modificar, apagar, restringir, transmitir ou se opor a determinados usos de suas informações. Se você tiver preocupações de privacidade quanto ao acesso ou à correção de seus dados pessoais, entre em contato com a secretaria de Recursos Humanos.

8.9 Informações

Para obter mais informações sobre retenção de Dados Pessoais ou qualquer aspecto desta Política, entre em contato com a Encarregada Geral de Proteção de Dados da Prefeitura que ajudará a direcionar/responder suas dúvidas.

8.10 Revisão da Política

Esta Política pode ser atualizada de tempos em tempos pela Prefeitura para refletir qualquer mudança na legislação ou nos métodos e práticas da Prefeitura. PAREI AQUI

9 LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS/PROCESSOS DE NÉGOCIO QUE TRATAM DADOS PESSOAIS

LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS/PROCESSOS DE NÉGOCIO QUE TRATAM DADOS PESSOAIS						
Controlador	Nome:		E-mail:		Endereço:	
	CEP:		Cidade:		Telefone:	
Encarregado	Nome:		E-mail:		Endereço:	
	CEP:		Cidade:		Telefone:	
Nome do serviço/processo de negócio	Nº Ref / ID	Data de Criação do Inventário	Data de Atualização do Inventário	Finalidade do tratamento dos dados pessoais	Trata Dados Pessoais Sensíveis?	

10 OS ENCARREGADOS SETORIAIS DEVERÃO FAZER A VERIFICAÇÃO DE CONFORMIDADE DO TRATAMENTO DE DADOS QUANTO AOS PRINCÍPIOS DA LGPD

Uma vez identificada(s) a(s) hipóteses de tratamento aplicável(is) às situações específicas de processamento de dados por órgãos e entidades da Administração Pública, deve-se partir para outras questões importantes para a verificação da conformidade quanto aos princípios da LGPD.

Para tanto, os Encarregados Setoriais do órgão ou entidade pública deverão analisar outras questões, detalhadas a seguir:

1. Identifique a finalidade para a qual o tratamento de dado é necessário. Os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade).

2. Defina como a finalidade do tratamento será informada ao titular, o que deve ser realizado antes do início do tratamento do dado (princípio da finalidade).

3. No caso de tratamento de dados que tenha sido iniciado antes da vigência da Lei, indique que providências serão tomadas para comunicar o titular sobre o tratamento realizado e a finalidade a qual se destina (princípio da finalidade).

4. Garanta que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação). Quaisquer mudanças na finalidade de tratamento deverão ser também comunicadas ao titular do dado.

5. Ao planejar a forma de tratamento de dados, atente para limitar a utilização ao mínimo de informações necessárias, garantindo abrangência pertinente e proporcional à consecução das finalidades informadas ao titular (princípio da necessidade).

6. Ao decidir realizar o tratamento de dados, defina antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso).

7. Garanta que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular (princípio do livre acesso).

8. Defina procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada (princípio da qualidade do dado).

9. Observe a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).

Observação: As unidades administrativas do Município de Rondonópolis deverão garantir o acesso às informações sobre o tratamento do dado do titular, resguardadas as informações de acesso restrito, conforme legislação vigente.

10. Defina e documente as medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança).

11. Identifique e registre as medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção).

12. Comprometa-se a não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).

13. Comprometa-se a adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas).

Para iniciar novos tratamentos de dados, é fundamental que unidades administrativas do Município de Rondonópolis analisem todas as questões citadas acima e documentem a forma de aplicação de cada um dos princípios da LGPD.

O Relatório de Impacto à Proteção de Dados Pessoais – RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição. Serve tanto para a análise quanto para a documentação.

A análise das questões acima deve também ser realizada para os casos de tratamento de dados anteriores à vigência da Lei. Nesses casos, é importante identificar os pontos de não conformidade com a LGPD, para os quais deverão ser elaborados planos para adaptação à Lei.

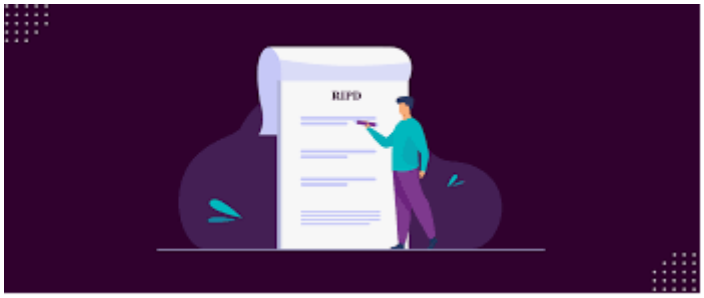
11 OS ENCARREGADOS SETORIAIS DE PROTEÇÃO DE DADOS DEVERÃO ELABORAR O RIPD – RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), em anexo, representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados. Segundo o inciso XVII do art. 5º da LGPD, o RIPD é documentação que deve ser mantida pelo Controlador dos dados pessoais.

> ***Art. 5º*** Para os fins desta Lei, considera-se:
> XVII – 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;

O seu conteúdo mínimo é indicado pelo parágrafo único do art. 38 da LGPD:

> ***Art. 38.*** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> ***Parágrafo único***. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotado



12 **REVISÃO DOS CONTRATOS EM CADA SECRETARIA**

Seguem sugestões de cláusulas contratuais de privacidade e proteção de dados pessoais a serem adotadas nas minutas de contrato padrão da Prefeitura.

Ressaltamos que a redação das cláusulas poderá ser alterada livremente pela Prefeitura, ao seu exclusivo critério, sendo certo que os dispositivos contratuais abaixo sugeridos destinam-se a permitir conformidade à LGPD.

Adicionalmente, é recomendável considerar o objeto do contrato e o nível de exposição da Prefeitura no tocante ao tratamento de dados pessoais no âmbito da relação contratual específica, de modo que seja efetivamente calibrada a necessidade de inserção e/ou refinamento das respectivas cláusulas.

Contratos com maior exposição ou com objeto mais sensível, naturalmente exigirão maior cuidado na redação de suas cláusulas. A análise deverá, sempre, ser individualizada e específica para cada instrumento, fornecedor, parceiro e/ou stakeholder, de modo que o contrato e as suas disposições preservem adequadamente as partes, vis a vis as interfaces apreciáveis no âmbito da LGPD e da cultura da privacidade.

Dessa forma, apresentamos a seguir duas sugestões de cláusulas: cláusula sumária e cláusula robusta.

É recomendado que, de acordo com o objeto de cada instrumento/contrato, seja realizada análise/assessment acerca da coleta, armazenagem e tratamento de dados pessoais no âmbito e escopo da respectiva relação contratual, de modo a permitir que se avalie qual das cláusulas abaixo colacionadas melhor se adequa ao correspondente objeto, mitigando assim eventuais exposições e riscos relacionados à Lei Geral de Proteção de Dados Pessoais.

13 SUGESTÃO DE QUESTIONÁRIO PARA PARCEIROS E FORNECEDORES

Prezado Parceiro,

Se você recebeu este questionário é porque foi convidado a colaborar com a Município De Rondonópolis – Estado De Mato Grosso, pessoa de direito público, situada à Avenida Duque De Caxias nº 1.000, Vila Aurora, no Município De Rondonópolis, Estado do Mato Grosso, inscrita no CNPJ sob o nº 03.347.101/0001-21 ("Prefeitura") e engajar-se numa cultura e ambiente de negócios onde os dados pessoais sejam devidamente protegidos, e o respeito aos direitos dos titulares seja considerado e preservado, nos termos da legislação vigente e das melhores práticas de Governança Corporativa.

Como você sabe, o mundo está em permanente evolução, sendo certo que a utilização e tratamento de dados pessoais merecem especial atenção à luz das alterações legislativas, bem como ante ao relevante desenvolvimento global da cultura da privacidade.

Nesse sentido, o Brasil estabeleceu parâmetros e regramentos relacionados ao tema - a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 – "LGPD").

A LGPD tem como principal objetivo regular o tratamento e a utilização de dados pessoais. Agora vamos entender um pouco mais sobre as novidades que esta legislação traz.

O que são dados pessoais?
Dados pessoais são qualquer informação relacionada a uma pessoa natural identificada ou identificável, como por exemplo, nome e sobrenome, endereço, telefone de contato, e-mail, ID profissional etc. O titular dos dados é a pessoa a quem os dados pessoais se referem.

O que são dados sensíveis?
Algumas categorias de dados pessoais são consideradas sensíveis e merecem uma atenção especial, podendo ser tratados apenas em hipóteses específicas, são eles: Dados sobre origem racial ou étnica; Opinião política; Convicções religiosas ou filosóficas; Dados genéticos; Dados biométricos; Dados de saúde; Filiação sindical; Dados sobre orientação sexual; Histórico criminal. E os dados de categoria especial: informações sobre menores de idade.

O que são dados de categoria especial?

Os dados de crianças e adolescentes são considerados dados pessoais de categoria especial, podendo ser tratados apenas em hipóteses específicas e levando em conta o seu melhor interesse.

Quem é o Controlador e o Operador?

O Controlador é a organização que possui relacionamento com os titulares dos dados e processa seus dados pessoais. Já o Operador é o terceiro que processa estes dados pessoais em nome do Controlador.

Por exemplo, imagine que a Empresa A coleta dados de seus clientes para prestar um determinado serviço. Após esta coleta de dados pessoais, a Empresa A envia os dados de seus clientes para a Empresa B, que analisa os dados e fornece estatísticas para que a Empresa A se organize com relação às novas campanhas que serão lançadas no mercado. Neste exemplo, a Empresa A seria o Controlador que recebe os dados de seus clientes (titulares dos dados) e a Empresa B seria o Operador, que processa estes dados a pedido da Empresa A (Controlador).

O que é tratamento de dados?

O tratamento de dados é 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.

Como os dados pessoais podem ser tratados?

A LGPD prevê algumas hipóteses para tratamento de dados pessoais em geral, são elas:

I. Execução de Contrato/Pré Contrato;
II. Cumprimento de obrigação legal ou regulatória;
III. Proteção da vida ou incolumidade física;
IV. Exercício regular de direitos;
V. Interesse legítimo;
VI. Consentimento;
VII. Execução de Políticas Públicas;
VIII. Estudos por órgãos de pesquisa;

IX. Tutela da saúde; e
X. Proteção de crédito.

Com relação ao consentimento, é importante ressaltar que a lei o conceitua como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Tendo em vista que a LGPD já se encontra em vigor, a Prefeitura adequou seus processos internos, em conformidade e aderência aos dispositivos legais.

Como forma de verificar a adequação de seus principais parceiros à LGPD, a Prefeitura elaborou este Questionário de Avaliação de Privacidade e Adequação à LGPD ("Questionário").
Neste sentido, você foi escolhido como um dos parceiros privilegiados, instados a colaborar conosco e com a disseminação da cultura da privacidade.

Lembramos que é muito importante que você nos forneça respostas completas e verídicas, para que possamos juntos verificar a melhor forma de adequar nossos processos/interfaces à LGPD, de forma a preservar a conformidade de todas as partes aos ditames vigentes. Assim, caso possua qualquer dúvida sobre as questões abaixo, por favor não deixe de nos contatar.
Estamos à disposição para conversar sobre o assunto.

Agradecemos sua colaboração e contamos com sua ajuda nesta trajetória!
Atenciosamente,

Prefeitura do Município de Rondonópolis

13.1 Questionário de avaliação de privacidade

Perguntas:

1 Descreva os dados pessoais que você recebe da Prefeitura e/ou transmite à Prefeitura e em quais circunstâncias.

2 Descreva os dados pessoais sensíveis que você recebe da Prefeitura e/ou transmite à Prefeitura e em quais circunstâncias.

3 Os dados pessoais recebidos da Prefeitura são acessados por terceiros (por exemplo, seus próprios prestadores de serviços/subcontratados/fornecedores terceirizados)? Em caso positivo, por favor detalhe em que circunstâncias.

4 Se respondeu 'sim' para a pergunta acima, especifique os terceiros e confirme quais medidas foram implementadas para cumprir as leis de proteção de dados, incluindo análise/due dilligence que você realizou ou pretende realizar com esses terceiros. Favor informar, inclusive, acerca da existência de acordos de confidencialidade (NDA) firmados com eventuais terceiros e/ou parceiros que tenham acesso a dados pessoais enviados e/ou recebidos da Prefeitura.

5 Você realiza tratamento de dados pessoais com fundamento nas bases legais e para cada atividade de tratamento, em conformidade com a LGPD? Favor especificar.

6 Você limita o processamento de dados pessoais ao tratamento necessário para os fins específicos que justificam a sua coleta? Favor exemplificar e especificar.

7 Você possui Registro das Operações de Tratamento de Dados Pessoais, conforme exigido pelo art. 37 da LGPD?

8 Você possui políticas de proteção de dados interna e externa? Se sim, por favor encaminhe uma cópia.

9 Você possui um Encarregado responsável pela área de proteção de dados pessoais?

10 O acesso a dados pessoais está restrito somente a funcionários autorizados? Quais as medidas implementadas para garantir o respeito por seus funcionários às suas políticas de proteção de dados? Favor indicar acerca da existência de acordos de confidencialidade e/ou cláusulas de confidencialidade nos respectivos contratos.

11 Quais são as medidas protetivas adotadas para garantir a segurança de dados pessoais (por exemplo, controles de acesso, criptografia, modificação de dados, mascaramento de dados, anonimização de dados, antivírus, firewalls, etc.)?

12 Os dados pessoais são armazenados em um local e ambiente seguros? Por favor, descreva como é feito o armazenamento.

13 Você possui mecanismos de segregação entre os dados fornecidos pela Prefeitura e aqueles que constam de sua base de dados? Se sim, por favor descreva-o.

14 Você possui as tecnologias e os processos necessários para responder às solicitações de acesso do titular de dados pessoais em conformidade com a LGPD? Existe algum protocolo e/ou procedimento para o tratamento de solicitações e/ou incidentes, em consonância à LGPD?

15 Você possui as tecnologias e os processos necessários para responder às solicitações do titular para exclusão de seus dados pessoais em conformidade com a LGPD e nos prazos legais estipulados?

16 Você possui as tecnologias e os processos necessários para atender ao direito de portabilidade do titular de dados pessoais em conformidade com a LGPD?

17 Você possui diferentes níveis de segurança da informação para dados sensíveis? Por favor, descreva-os.

18 Caso os serviços solicitados exijam atividades de tratamento que resultem em um alto risco para os titulares de dados, você realiza um Relatório de Impacto à Proteção de Dados Pessoais nos serviços solicitados?

19 Você possui salvaguardas/mecanismos adequados, em conformidade com a LGPD, para o armazenamento e/ou transferência internacional de dados pessoais?

20 Você anonimiza dados pessoais e sensíveis mediante encriptação ou remoção de informações que tornam uma pessoa natural identificada ou identificável?

21 Seu processamento inclui automatização de qualquer tomada de decisão, criação de perfis com base nos dados pessoais transferidos (profiling) ou utilização analítica (analytics)?

22 Caso você colete dados pessoais, você fornece informações sobre o tratamento de dados aos titulares (incluindo clientes, pessoal, etc.), em conformidade com o artigo 9º da LGPD?

23 Caso você obtenha dados pessoais de titulares através de consentimento, o consentimento é obtido de acordo com as estipulações da LGPD? Os consentimentos são devidamente armazenados, nos termos da LGPD?

24 Você possui contratos compatíveis com as leis de proteção de dados, em vigor, com seus fornecedores e parceiros?

25 Você oferece orientação aos funcionários de terceiros a respeito das práticas a serem tomadas em relação à proteção de dados pessoais? Se sim, forneça uma cópia das instruções enviadas a terceiros envolvidos no processamento de dados destinados/enviados pela Prefeitura.

26 Você exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e segurança de dados?

27 Você instrui seus funcionários e contratados a limitar o armazenamento de dados pessoais do cliente em dispositivos de armazenamento móvel ao mínimo exigido para fins comerciais? Os seus colaboradores e fornecedores encontram-se aderentes à LGPD, bem como às melhores práticas de tratamento, coleta e armazenagem de dados pessoais? Existe algum tipo de auditoria/confirmação que seja realizada perante os vossos colaboradores/fornecedores para verificação da aderência e conformidade aos dispositivos da LGPD?

28 Você possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais? Se sim, forneça uma cópia.

29 Você conduz avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?

30 Você será capaz de atender solicitações da Prefeitura para remover dados pessoais de seus sistemas, se necessário? Se sim, dentro de qual prazo?

31 Se respondeu “sim” para a pergunta acima, especifique o procedimento para descarte de dados.

32 Você - em relação aos serviços solicitados - é capaz de detectar incidentes de segurança (incluindo acesso não autorizado, destruição, perda, alteração e violações de dados)?

33 Você possui um procedimento para agir, prontamente, em caso de incidentes de segurança, incluindo notificação aos titulares de dados afetados e à Prefeitura? Se sim, descreva-o.

34 Se respondeu 'sim' para a pergunta acima, especifique os terceiros e confirme quais medidas foram implementadas para cumprir as leis de proteção de dados, incluindo análise/due diligence que você realizou ou pretende realizar com esses terceiros.

35 Você transfere dados do cliente para outro país? Se sim, é a transferência interna/externa? Por favor, forneça uma cópia das medidas de segurança tomadas e contrato.

36 Você possui uma política/procedimento de back-up em relação aos dados pessoais? Se sim, por favor, forneça uma cópia para revisão.

37 Você contratou algum serviço de assessoria para implementação da LGPD? Quais as medidas que estão sendo adotadas para regularização?

38 Sua empresa já passou por algum incidente de violações de segurança da informação nos últimos dois (2) anos? Se sim, quais foram as circunstâncias em que a violação ocorreu e quais medidas foram adotadas para evitar novos incidentes?

39 Sua empresa está atualmente sujeita a quaisquer ações de execução, investigações ou litígios relacionados à privacidade ou à segurança da informação? Em caso afirmativo, por favor indique sobre quais circunstâncias e forneça cópias de documentos mais relevantes.

40 A empresa é certificada em algum padrão ou framework de segurança? Se sim, quais são eles?

* Quando solicitadas evidências solicitamos, por gentileza, que sejam enviadas em um padrão de nomenclatura, para facilitar a identificação (e.g., #_Nome do arquivo, onde ## corresponde ao número da pergunta).

Disposições Gerais

Ao responder este Questionário, a empresa respondente garante à Prefeitura que:

I. O signatário deste Questionário detém todos os poderes e informações necessários para respondê-lo, bem como todos os poderes para representar a empresa no âmbito deste Questionário;

II. Todas as informações fornecidas pela empresa são verdadeiras, responsabilizando-se por qualquer omissão, informação incorreta ou incompleta contida neste Questionário;

III. Caso ocorram alterações às respostas fornecidas neste Questionário, a empresa se compromete a informar a Prefeitura tão logo seja possível.

As informações fornecidas neste Questionário são reputadas confidenciais.

As partes comprometem-se a manter completa confidencialidade e sigilo sobre quaisquer dados ou informações trocadas no bojo deste Questionário, não as divulgando ou transferindo a terceiros sem a devida e expressa autorização da outra parte. As partes exercerão medidas de segurança e grau de cuidado com as informações confidenciais recebidas não inferior àqueles que seriam aplicados às suas próprias informações confidenciais, garantindo proteção adequada contra qualquer divulgação, cópia ou utilização não autorizada.

Não serão reputadas informações confidenciais as informações que:

I. Estejam ou venham a tornar-se de domínio público de outra forma que não em função da revelação deste Questionário;
II. Comprovadamente já estivessem na posse da parte receptora por conta de ter sido registrada em seus arquivos ou que já estivesse em uso antes do seu recebimento pela parte divulgadora e que não estivessem cobertas por obrigação de confidencialidade; ou
III. Tenham sido recebidas de um terceiro de boa-fé, não tendo recebido a informação diretamente ou indiretamente da parte divulgadora.

Não serão consideradas quebra à obrigação de confidencialidade a divulgação de informações exigidas por lei ou por autoridade policial, judicial ou administrativa, ordem judicial ou regulamento aplicável a parte receptora. Caso a parte receptora seja demandada a divulgar dados pessoais ou informações confidenciais vinculadas à outra parte, recebidos por meio deste Questionário, a parte receptora deverá informar imediatamente a parte divulgadora para que possa tomar as medidas cabíveis.

A Prefeitura se reserva ao direito de realizar inspeções e avaliações sobre os níveis de proteção de dados pessoais adotados por seus parceiros sempre que julgar necessário. Estas avaliações poderão compreender análise de documentos solicitados, solicitação de informações e auditorias. As partes se comprometem a envidar seus melhores esforços para colaborar uma com a outra em procedimentos de verificação de nível de proteção de dados pessoais e adequação às legislações vigentes, especialmente à LGPD, sempre com vistas a permitir integral conformidade às melhores práticas de Governança Corporativa.

As garantias e obrigações estabelecidas neste Questionário passarão a vigorar a partir da data de sua assinatura e permanecerão em vigor por prazo indeterminado. Caso as informações deste Questionário sejam atualizadas, conforme as condições estabelecidas nas Disposições Gerais deste Questionário se aplicarão também às novas informações confidenciais complementares.
Rondonópolis, [Data]

_____ [nome da empresa terceira]

* Por favor, peça a um representante da empresa para assinar a última página e rubricar as demais páginas deste Questionário.

ANEXOS

ANEXO 1 - SUGESTÃO DE CLÁUSULAS SUMÁRIAS - PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A Contratada compromete-se a:

I. cumprir com as obrigações e requisitos das legislações de proteção de informações relacionadas a pessoa natural identificada ou identificável ("Dados Pessoais") vigentes, incluindo, mas não se limitando à Lei no 13.709, de 14 de agosto de 2018 ("Lei Geral de Proteção de Dados Pessoais"), Lei no 12.965, de 23 de abril de 2014 ("Marco Civil da Internet"), Lei no 8.078, de 11 de setembro de 1990 ("Código de Defesa do Consumidor"), Lei Complementar no 166, de 08 de abril de 2019 ("Lei do Cadastro Positivo"), Lei no 12.527, de 18 de novembro de 2011 ("Lei de Acesso à Informação"), Decreto no 7.962, de 15 de março de 2013 ("Decreto Comércio Eletrônico" e Decreto nº 10.789 de 11 de abril de 2022 ("Regulamentação da Lei 13.709/2018"), conforme aplicável ("Legislações de Proteção de Dados Pessoais");

II. Abster-se de realizar quaisquer ações ou omissões que possam resultar de alguma forma em violação das Legislações de Proteção de Dados Pessoais;

III. Tomar todas as medidas razoavelmente necessárias para manter-se em conformidade com as Legislações de Proteção de Dados Pessoais;

IV. Garantir que qualquer atividade realizada que utilize 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 ("Tratamento") resultante do objeto do presente Contrato, bem como o uso e marketing de tais dados, e as medidas adotadas para a privacidade e segurança estejam em conformidade com as Legislações de Proteção de Dados Pessoais e sejam consistentes com a Política de Privacidade da Prefeitura de Rondonópolis, conforme disposto em seu site em http://www.rondonopolis.mt.gov.br/, a qual poderá ser atualizada a qualquer tempo pela Prefeitura visando conformidade com a legislação brasileira e internacional de proteção de dados pessoais;

V. Não realizar qualquer Tratamento de Dados Pessoais, resultantes da execução do Contrato, sem enquadramento em uma das bases legais estipuladas no art. 7º da LGPD;

VI. Adotar medidas técnicas e organizacionais adequadas para garantir a segurança dos Dados Pessoais;

VII. Somente realizar o Tratamento de Dados Pessoas como resultado do presente Contrato com a finalidade de cumprir com as respectivas obrigações contratuais;

VIII. Não permitir ou facilitar o Tratamento de Dados Pessoais por terceiros para qualquer finalidade que não seja o cumprimento de suas respectivas obrigações contratuais; e

IX. Comunicar a Prefeitura imediatamente e em prazo não superior a 24 (vinte e quatro) horas em caso de incidentes e/ou vazamentos envolvendo dados resultantes do tratamento de Dados Pessoais obtidos para a execução do presente Contrato.

RESPONSABILIDADE

A Contratada, desde já reconhece e declara que o descumprimento de qualquer Legislação de Proteção de Dados Pessoais, das políticas da Prefeitura ou das provisões contidas nesta cláusula gerará obrigação da Contratada em indenizar, defender e manter a Prefeitura, suas unidades administrativas, conselheiros, secretários, diretores, executivos e servidores isentos de todas e quaisquer responsabilidades, perdas, os danos, prejuízos, custos, despesas, ações, processos, demandas, multas e penalidades decorrentes do descumprimento de suas obrigações, declarações e garantias previstas nesta Cláusula, sendo que nenhuma limitação de responsabilidade eventualmente acordada neste Contrato será aplicada para as indenizações por descumprimento das obrigações desta Cláusula."

ANEXO II - SUGESTÃO DE CLÁUSULAS ROBUSTAS – PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

OBJETIVO

Este Anexo estabelece as obrigações e responsabilidades do [Fornecedor], no que se refere à observância das obrigações e requisitos das Legislações de Proteção de Dados Pessoais.

DEFINIÇÕES

Para os fins deste Anexo, devem ser consideradas as seguintes definições e descrições para seu melhor entendimento:

I. Autoridade Nacional - significa a Autoridade Nacional de Proteção de Dados ou órgão da administração pública que venha a substituí-la;

II. Controlador - significa o Município de Rondonópolis – Estado De Mato Grosso, pessoa de direito público, situada à Avenida Duque De Caxias nº 1.000, Vila Aurora, no Município De Rondonópolis, Estado do Mato Grosso, inscrita no CNPJ sob o nº 03.347.101/0001-21;

III. Dado Pessoal - significa qualquer informação relacionada a pessoa natural identificada ou identificável;

IV. Dado Pessoal Sensível" significa 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;

V. Leis de Proteção de Dados Pessoais - significam as legislações de proteção de Dados Pessoais vigentes, incluindo, mas não se limitando à Lei no 13.709, de 14 de agosto de 2018 ("LGPD"), Lei no 12.965, de 23 de abril de 2014 ("Marco Civil da Internet"), Lei no 8.078, de 11 de setembro de 1990 ("Código de Defesa do Consumidor"), Lei Complementar no 166, de 08 de abril de 2019 ("Lei do Cadastro Positivo"), Lei no 12.527, de 18 de novembro de 2011 ("Lei de Acesso à Informação") e Decreto no 7.962, de 15 de março de 2013 ("Decreto Comércio Eletrônico");

VI. Operador – significa pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

VII. Tratamento - significa qualquer 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; e

VIII. Titular - significa pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.

Todas as definições acima deverão ser interpretadas nos termos das Leis de Proteção de Dados Pessoais. Caso algum termo seja utilizado neste instrumento e não esteja compreendido nesta cláusula, as Partes deverão adotar a definição estipulada nas Leis de Proteção de Dados.

OBRIGAÇÕES DO OPERADOR

O Operador se compromete nos seguintes termos:

I. Adotar as medidas técnicas e organizacionais adequadas para proteger os Dados Pessoais, cujo nível de segurança seja adequado ao risco decorrente do Tratamento e da natureza dos Dados Pessoais a serem protegidos, contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado ou ilícito;

II. Tratar os Dados Pessoais disponibilizados pelo Controlador em conformidade com as suas instruções, as cláusulas do presente Anexo e as Leis de Proteção de Dados Pessoais, sendo certo que caso não possa cumprir estas obrigações por qualquer razão, concorda em informar imediatamente o Controlador desse fato, tendo neste caso o Controlador o direito de suspender o compartilhamento dos Dados Pessoais e/ou de rescindir o Contrato, sem prejuízo da apuração das eventuais perdas e danos em favor do Controlador;

III. Dispor de procedimentos necessários para que terceiros autorizados a acessar os Dados Pessoais, incluindo os subcontratantes, respeitem e mantenham a confidencialidade e a segurança dos Dados Pessoais. Todas as pessoas sob a autoridade do Operador, incluindo os subcontratantes, devem ser obrigados a tratar os Dados Pessoais apenas sob a orientação do

Operador, bem como a cumprir as obrigações contratuais e legais referentes ao tema, sob pena de arcar isolada e integralmente com as responsabilidades e danos decorrentes da violação ou incidente;

IV. Notificar imediatamente o Controlador e em prazo nunca superior a 24 (vinte e quatro) horas no que diz respeito a:

a. Qualquer intimação, pedido, requisição de cooperação judicial no que diz respeito a divulgação de Dados Pessoais, a não ser que exista alguma proibição em contrário, como uma proibição prevista para preservar a confidencialidade de uma investigação policial;

b. Qualquer acesso acidental ou não autorizado; e

c. Qualquer solicitação de acesso realizada diretamente pelo Titular, sem respondê-la, a não ser que tenha sido autorizado a fazê-lo;

V. Tratar os Dados Pessoais estritamente para os fins dispostos na cláusula 7.1 abaixo e possuir legitimidade para oferecer as garantias e cumprir as obrigações estabelecidas nas presentes cláusulas;

VI. Indicar ao Controlador um setor profissional capacitado a responder às consultas relativas ao Tratamento de Dados Pessoais e cooperar de boa-fé com o Controlador, os Titulares e a Autoridade Nacional em todas as eventuais consultas, obrigatoriamente dentro do prazo legal aplicável, sob pena de arcar isolada e integralmente com as responsabilidades e danos decorrentes da violação ou incidente;

VII. A pedido do Operador, fornecer-lhe-á provas que demonstrem que dispõe dos recursos técnicos e financeiros necessários para cumprir às obrigações e responsabilidades estipuladas na presente Cláusula;

VIII. A pedido do Controlador, facilitar/disponibilizar o acesso às suas instalações de Tratamento de Dados Pessoais, aos seus bancos de dados e a toda a documentação necessária para o Tratamento para fins de revisão, auditoria ou certificação, a ser realiza pelo Controlador (ou por qualquer inspetor ou auditor imparcial e independente escolhido pelo Controlador e a que o Operador não se tenha oposto em termos razoáveis), para determinar se são cumpridas as garantias e as obrigações previstas nas presentes cláusulas, mediante notificação e durante as horas de trabalho habituais;

IX. Não divulgar nem transferir Dados Pessoais a terceiros responsáveis pelo Tratamento de Dados Pessoais estabelecidos em países que não possuam regime de proteção de Dados Pessoais compatível com os termos deste Anexo e as Leis de Proteção de Dados

Pessoais, sob pena de arcar isolada e integralmente com as responsabilidades e danos decorrentes da violação ou incidente;

X. No que tange às transferências posteriores de Dados Sensíveis, garantir que os Titulares deem o seu consentimento inequívoco para esse efeito, nos termos da Lei, sob pena de arcar isolada e integralmente com as responsabilidades e danos decorrentes da violação ou incidente; e

XI. Manter o Controlador informado sobre todas as subcontratações existentes, atualizando de forma célere quando houverem novas contratações, devendo os eventuais terceiros e/ou subcontratados aderirem integralmente às disposições deste instrumento, sem prejuízo da observância integral das normas nacionais e internacionais referentes ao Tratamento, coleta e armazenamento de dados pessoais e segurança da informação;

RESPONSABILIDADE

O Operador desde já reconhece e declara que o descumprimento de qualquer Legislação de Proteção de Dados Pessoais, das políticas do Controlador ou das provisões contidas nesta Cláusula gerará obrigação do Operador em indenizar, defender e manter o Controlador, suas entidades afiliadas, conselheiros, diretores, executivos e empregados isentos de todas e quaisquer responsabilidades, perdas, os danos, prejuízos, custos, despesas, ações, processos, demandas, multas e penalidades decorrentes do descumprimento de suas obrigações, declarações e garantias previstas nesta Cláusula, sendo que nenhuma limitação de responsabilidade eventualmente acordada neste Anexo será aplicada para as indenizações por descumprimento das obrigações desta Cláusula.

O Operador não poderá, em hipótese alguma, invocar o descumprimento das disposições contratuais e Legislações de Proteção de Dados por subcontratante para eximir-se de suas responsabilidades assumidas no presente Anexo e nesta Cláusula.

SUBCONTRATAÇÃO

O Operador não poderá subcontratará nenhuma das suas atividades de Tratamento executadas por conta do Controlador nos termos do presente Anexo sem o prévio e formal consentimento deste, devendo tal consentimento ser manifestado por escrito e subscritado por quem de direito. Sempre que o Operador subcontratar as suas obrigações aqui dispostas, com o

consentimento do Controlador, fará apenas mediante contrato por escrito com o subcontratante que imponha a este último as mesmas obrigações no que tange à proteção de dados pessoais dispostas no presente Anexo. Em caso de descumprimento pelo subcontratante das obrigações em matéria de proteção de Dados Pessoais que lhe incumbem nos termos do referido contrato por escrito, o Operador continua a ser plenamente responsável perante o Controlador pelo cumprimento destas obrigações;

AUDITORIA E SUPERVISÃO

O Operador permitirá que o Controlador, seus auditores internos e auditores independentes, inspetores, regulamentadores e outros representantes, acessem:

I. A quaisquer instalações pertencentes ou geridas pelo Operador na qual o Operador forneça os serviços objeto do presente Anexo;

II. Ao pessoal pertinente do Operador;

III. Aos subcontratados;

IV. A sistemas de computação de dados e registros relacionados ao Tratamento de Dados Pessoais, com a finalidade de realizar auditorias do Operador ou quaisquer de seus subcontratados para verificar a conformidade do Operador em relação ao cumprimento da LGPD.

O Operador deverá dar plena cooperação ao Controlador e a seus representantes na realização de auditorias. O Controlador poderá executar as auditorias quando entender necessário, sem qualquer limitação. Para a realização de auditorias o Controlador comunicará por escrito com antecedência de 15 (quinze) dias.

O Operador atenderá, por escrito, no prazo de 15 (quinze) dias todas as recomendações que o Controlador vier a fornecer, bem como as regularizações resultantes das referidas auditorias.

O Operador deverá:

I. Manter organizada toda documentação relativa ao Tratamento de Dados Pessoais referentes aos Dados Pessoais disponibilizadas pelo Operador;

II. Fornecer ao Controlador, mediante solicitação por qualquer meio, cópias de todos os registros das atividades de Tratamento de Dados Pessoais, dentro do prazo estipulado pelo Controlador;

III. Fornecer ao Controlador cópia do relatório de auditoria do Operador mais recente na ocasião ou análise relacionada a qualquer Tratamento de Dados Pessoais, dentro do prazo estipulado pelo Controlador; e

IV. Fornecerá ao Controlador cópias dos relatórios resultantes de quaisquer auditorias realizadas pelo pessoal interno/externo do Operador que incluam Tratamento de Dados Pessoais em seu escopo.

Cooperação com o Controlador.

I. Se o Controlador determinar que a LGPD ou a política do Controlador necessitam de avaliação dos impactos sobre a privacidade de qualquer Tratamento de Dados Pessoais, o Operador deverá cooperar plenamente para a sua realização e eventuais melhorias;

II. Se o Controlador determinar que a LGPD ou a política do Controlador exigem que o Controlador busque orientação ou consulte terceiros, inclusive qualquer autoridade governamental ou representante de órgão trabalhista, a respeito do Tratamento de Dados Pessoais pelo Operador, deverá haver a cooperação do Operador, nos exatos termos e prazos estipulados pelo Controlador;

III. O Operador deverá comunicar o Controlador, em até 24 (vinte e quatro) horas contadas da respectiva ciência, acerca da iminência e do início de procedimento de fiscalização, reclamação, investigação, auditoria, ação ou de cumprimento de obrigações decorrente ou relacionado ao Tratamento de Dados Pessoais a ser realizada por autoridades governamentais;

IV. Em razão do item anterior o Operador deverá cooperar plenamente com o Controlador em qualquer processo de reclamação, investigação, auditoria, ação ou execução decorrente ou relacionado com o Tratamento de Dados Pessoais;

V. A título de cooperação, o Operador deverá dar acesso a informações, registros, de todo e qualquer empregado, preposto ou terceiro contratado do Operador envolvido no Tratamento de Dados Pessoais.

DISPOSIÇÕES GERAIS

Finalidade – As Partes acordam que o Tratamento de Dados Pessoais resultante do presente Anexo será realizado estritamente para os fins de [indicar objeto do Contrato].

Prazo de Guarda dos Dados Pessoais – O Operador irá armazenar os Dados Pessoais dos Titulares pelo prazo necessário para cumprimento do Contrato, sendo que após o término

de sua vigência manterá somente os Dados Pessoais necessários para cumprimento de suas obrigações legais.

Eliminação de Dados Pessoais – As Partes acordam que após o término do Tratamento de Dados Pessoais estipulado no Contrato, o Operador e os subcontratados deverão, à escolha do Controlador, devolver todos os Dados Pessoais transferidos e suas respectivas cópias ao Controlador ou deverão destruir todos os Dados Pessoais e certificar ao Controlador que o mesmo foi realizado, a não ser que exista obrigação legal do Operador que o impeça de devolver ou destruir os Dados Pessoais transferidos. Neste caso, o Operador declara que irá garantir a confidencialidade dos Dados Pessoais transferidos e cessará qualquer tipo de Tratamento dos Dados Pessoais, sob pena de arcar isolada e integralmente com as responsabilidades e danos decorrentes da violação ou incidente.

Segurança – Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do Tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades de Titulares. O Operador e quaisquer subcontratados deverão manter os mesmos níveis de segurança para proteção de Dados Pessoais recomendados pelo Controlador.

Caso quaisquer eventuais alterações nas Leis de Proteção de Dados, regulamentos ou recomendações da Autoridade Nacional, que venham a ocorrer durante a duração do Contrato, resultarem na desconformidade do Anexo com as determinações das Leis de Proteção de Dados, as Partes deverão empenhar seus melhores esforços de forma conjunta, para implementar todas e quaisquer eventuais atualizações e refinamentos no Anexo que se fizerem necessárias, no prazo de até 30 (trinta) dias contados da vigência da eventual alteração nas Leis de Proteção de Dados, regulamentos ou recomendações da Autoridade Nacional.

ANEXO III - MODELO DE TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

O <u>Município de Rondonópolis-Estado de Mato Grosso</u>, pessoa jurídica de direito público, inscrita no CNPJ sob n.º 03.347.101/0001-21, com sede à Avenida Duque de Caxias, nº 1.000, Vila Aurora, nesta cidade, no município de Rondonópolis - MT, sendo neste ato representada pelo seu Prefeito Municipal o Sr:xxxxxxx, doravante denominado CONTRATANTE, e, de outro lado, a (NOME DA EMPRESA), sediada em (ENDEREÇO), CNPJ n.° (CNPJ), doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º DD/AAAA doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Privacidade da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis, confidenciais e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 10.789 de 11 de Abril de 2022 – Regulamentação da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I - Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II - Informação Pública ou Ostensiva: é aquela cujo acesso é irrestrito, obtida por meio de divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III - Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV - Informações Confidenciais e Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como

aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V - Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES CONFIDENCIAIS E SIGILOSAS

Serão consideradas como informação confidencial e sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES.

Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da eqüidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas

neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessária a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da (CIDADE DA CONTRATANTE), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja. E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

De Acordo

_____	_____
Contratante (Nome do Contratante) (Matrícula)	Contratada (Nome da Contratada) (Qualificação)
_____	_____
Testemunha 1 (Nome) (Qualificação	Testemunha 2 (Nome) (Qualificação)

Rondonópolis-MT, XXXXXX, de XXXXXX de 202X

ANEXO IV - MODELO DE TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, POLÍTICA DE PRIVACIDADE, SUAS NORMAS E PROCEDIMENTOS

1. Identificação do usuário interno ou externo

Nome:	
RG/CPF:	
Matrícula:	
Órgão/Empresa (nome e CNPJ, somente para EMPRESAS OU ÓRGÃOS EXTERNOS:	

Estou ciente da existência da Política de Segurança da Informação, Política de Privacidade, normas e procedimentos do Município de Rondonópolis.

Comprometo-me a:

a) Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança da Informação, Política de Privacidade, com as Normas, Manuais e procedimentos vigentes do Município de Rondonópolis; e
b) Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.

Rondonópolis-MT, XXXXXX, de XXXXXX de 202X

_____
Assinatura do Usuário(a)

ANEXO V - MODELO DE TERMO DE CIÊNCIA

1. FINALIDADE

1.1. Este documento tem como finalidade obter comprometimento formal dos empregados da contratada diretamente envolvidos nos projeto sobre o conhecimento da declaração e manutenção de sigilo e das normas de segurança vigentes na PREFEITURA DE RONDONÓPOLIS.

2. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO.

Contrato nº:			
Objeto:			
Gestor do Contrato:		**Matrícula**	
Contratante:		**CNPJ**	
Contratada:		**CPF**	
Preposto da Contratada:			

3. CIÊNCIA E APROVAÇÃO

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

_____ (Nome) – (Matrícula) Preposto da Contratada	_____ (Nome) – (Matrícula) Preposto da Contratada	_____ (Nome) – (Matrícula) Funcionário
_____ (Nome) – (Matrícula) Preposto da Contratada	_____ (Nome) – (Matrícula) Preposto da Contratada	_____ (Nome) – (Matrícula) Preposto da Contratada

Rondonópolis-MT, XXXXXX, de XXXXXX de 202X

ANEXO VI - MODELO DE TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Ao assinar o presente termo, o Titular Sr.(a) _____, inscrito (a) no CPF sob n°_____ e RG nº _____ consente e concorda que o **MUNICÍPIO DE RONDONÓPOLIS-ESTADO DE MATO GROSSO**, pessoa jurídica de direito público, inscrita no CNPJ sob n.º 03.347.101/0001-21, com sede à Avenida Duque de Caxias, nº 1.000, Vila Aurora, nesta cidade, no município de Rondonópolis - MT, sendo neste ato representada pelo seu Prefeito Municipal o Sr:xxxxxxx, doravante denominado CONTROLADOR, tome decisões referentes ao tratamento de seus dados pessoais e dados pessoais sensíveis, de acordo com os artigos 7° e 11 da Lei n° 13.709/2018, bem como realize o tratamento de tais dados, envolvendo operação realizada com dados pessoais e dados pessoais sensíveis, 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.

CLÁUSULA PRIMEIRA - Dados Pessoais

O Titular autoriza o(a) Controlador(a) a realizar o tratamento, ou seja, a utilizar os seguintes dados pessoais, para os fins que serão relacionados na cláusula segunda:

Exemplo: Informar os dados que serão disponibilizados, como por exemplo, Nome completo; Data de nascimento; – Número e imagem da Carteira de Identidade (RG); – Número e Imagem do Cadastro de Pessoas Físicas (CPF) ou Carteira Nacional de Habilitação (CNH); – Imagem da Certidão de Nascimento (quando utilizada como documento para menores de idade); – Número e imagem da Carteira de Registro Profissional; Número e imagem do Título de Eleitor; Número e Imagem da Certidão de Casamento Civil ou Religioso ou Instrumento de União Estável lavrado em Cartório ou Declaração de União Estável - Imagem do Cartão de vacinação; - Tipo Sanguíneo; - Imagem do Laudo médico; – Imagem do Atestado Médico; Foto; Dados financeiros; Imagem do Diploma, histórico escolar e/ou declaração dos níveis de instrução ou escolaridade; imagem e Endereço com CEP; Números de telefones, WhatsApp e endereços de e-mail; Banco, agência e número de contas bancárias; (relacionar outros documentos específicos exigidos pela secretaria).

CLÁUSULA SEGUNDA - Finalidade do Tratamento dos Dados

O Titular autoriza que o(a) Controlador(a) utilize os dados pessoais e dados pessoais sensíveis listados neste termo para as seguintes finalidades:

Exemplo: Informar a finalidade, como por exemplo, para cumprimento, pela Controladora, de obrigações impostas por órgãos de fiscalização; A pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiros; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Parágrafo Primeiro: Caso seja necessário o compartilhamento de dados com terceiros que não tenham sido relacionados nesse termo ou qualquer alteração contratual posterior, será ajustado

novo termo de consentimento para este fim (§ 6° do artigo 8° e § 2° do artigo 9° da Lei n° 13.709/2018).

Parágrafo Segundo: Em caso de alteração na finalidade, que esteja em desacordo com o consentimento original, a Controladora deverá comunicar o Titular, que poderá revogar o consentimento, conforme previsto na cláusula sexta.

CLÁUSULA TERCEIRA - Compartilhamento de Dados

A Controladora fica autorizada a compartilhar os dados pessoais do Titular com outros agentes de tratamento de dados, caso seja necessário para as finalidades listadas neste instrumento, desde que, sejam respeitados os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

CLÁUSULA QUARTA - Responsabilidade pela Segurança dos Dados

O Controlador responsabiliza-se pela manutenção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

O Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD), conforme art. 48 da Lei nº 13709/2018, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

O Controlador poderá manter e tratar os dados pessoais do Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades listadas neste termo.

Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido.

CLÁUSULA OITAVA - Vazamento de Dados ou Acessos Não Autorizados – Penalidades

As partes poderão entrar em acordo, quanto aos eventuais danos causados, caso exista o vazamento de dados pessoais ou acessos não autorizados, e caso não haja acordo, a Controladora tem ciência que estará sujeita às penalidades previstas no artigo 52 da Lei n° 13.709/2018.

Rondonópolis-MT, _____/_____/_____.

_____

Assinatura do Titular

ANEXO VII - INVENTÁRIO DE DADOS PESSOAIS						
Essa guia é um modelo de um formulário operacional a ser reproduzido, adaptado e preenchido de acordo com a sua atividade de tratamento de dados pessoais. São fornecidos comentários adicionais como notas para auxiliar no preenchimento do formulário.						
1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais						
1.1 - Nome do serviço / Processo de negócio						
1.2 - Nº Referência / ID						
1.3 - Data de Criação do Inventário						
1.4 - Data Atualização do Inventário						
2 - Agentes de Tratamento e Encarregado	Nome	Endereço		CEP	Telefone	E-mail
2.1 – Controlador						
2.2 – Encarregado						
2.3 - Operador						
3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação	

3.1 - Em qual fase do ciclo de vida o Operador atua					
4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados					
4.1 - Descrição do Fluxo do tratamento dos dados pessoais					
5 - Escopo e Natureza dos Dados Pessoais					
5.1 - Abrangência da área geográfica do tratamento					
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais					
6 - Finalidade do Tratamento de Dados Pessoais					
6.1 - Hipótese de Tratamento					
6.2 - Finalidade					
6.3 - Previsão legal					
6.4 - Resultados pretendidos para o titular de dados					

6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo				
7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				
7.2 -Dados Financeiros	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.2.1 - Dados de identificação financeira				
7.2.2 - Recursos financeiros				

7.2.3 - Dívidas e despesas				
7.2.4 - Situação financeira (Solvência)				
7.2.5 - Empréstimos, hipotecas, linhas de crédito				
7.2.6 - Assistência financeira				
7.2.7 - Detalhes da apólice de seguro				
7.2.8 - Detalhes do plano de pensão				
7.2.9 - Transações financeiras				
7.2.10 - Compensação				
7.2.11 - Atividades profissionais				
7.2.12 - Acordos e ajustes				
7.2.13 - Autorizações ou consentimentos				
7.3 - Características Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.3.1 - Detalhes pessoais				

7.3.2 - Detalhes militares				
7.3.3 - Situação de Imigração				
7.3.4 - Descrição Física				
7.4 - Hábitos Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.4.1 - Hábitos				
7.4.2 - Estilo de vida				
7.4.3 - Viagens e deslocamentos				
7.4.4 - Contatos sociais				
7.4.5 - Posses				
7.4.6 - Denúncias, incidentes ou acidentes				
7.4.7 - Distinções				
7.4.8 - Uso de mídia				
7.5 - Características Psicológicas	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.5.1 - Descrição Psicológica				

7.6 - Composição Familiar	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.6.1 - Casamento ou forma atual de coabitação				
7.6.2 - Histórico conjugal				
7.6.3 - Familiares ou membros da família				
7.7 - Interesses de lazer	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.7.1 - Atividades e interesses de lazer				
7.8 - Associações	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)				
7.9 - Processo Judicial/Administrativo/Criminal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados

7.9.1 - Suspeitas				
7.9.2 - Condenações e sentenças				
7.9.3 - Ações judiciais				
7.9.4 - Penalidades Administrativas				
7.10 - Hábitos de Consumo	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.10.1 - Dados de bens e serviços				
7.11 - Dados Residenciais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.11.1 - Residência				
7.12 - Educação e Treinamento	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.12.1 - Dados acadêmicos/escolares				
7.12.2 Registros financeiros do curso/treinamento				
7.12.3 - Qualificação e experiência profissional				

7.13 - Profissão e emprego	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.13.1 - Emprego atual				
7.13.2 - Recrutamento				
7.13.3 - Rescisão de trabalho				
7.13.4 - Carreira				
7.13.5 - Absentismo e disciplina				
7.13.6 -Avaliação de Desempenho				
7.14 -Registros/gravações de vídeo, imagem e voz	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.14.1 - Vídeo e imagem				
7.14.2 - Imagem de Vigilância				
7.14.3 - Voz				
7.15 -Outros (Especificar)	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.15.1 - Outros (Especificar)				

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou ética				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

9 - Frequência e totalização das categorias de dados pessoais tratados		
9.1 - Frequência de tratamento dos dados pessoais		
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados		
10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		
11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1		
11.2 - Nome da Instituição 2		

11.3 - Nome da Instituição 3			
11.4 - Nome da Instituição 4			
12 - Medidas de Segurança/Privacidade	Tipo de medida de segurança e privacidade		Descrição do(s) Controle(s)
12.3 - Medida de Segurança/Privacidade 1			
12.2 - Medida de Segurança/Privacidade 2			
12.3 - Medida de Segurança/Privacidade 3			
13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			
14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Processo Contratação	Objeto do Contrato	E-mail do Gestor do Contrato

14.2 - Contrato nº 1			
14.2 - Contrato nº 2			

ANEXO VIII - MODELO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

PREFEITURA MUNICIPAL DE RONDONÓPOLIS

SECRETARIA MUNICIPAL DE XXXXXX

Nome do DPO (Encarregado Geral)

Nome do Encarregado Setorial (Titular e Suplente)

Data

Cidade

1. Da necessidade do presente Relatório de Impacto à Proteção de Dados Pessoais

Explique o objetivo do projeto e quais tratamentos são necessários para isso. Demonstre por que a organização achou necessário a realização de um RIPD.

2. Descrição do(s) tratamento(s)

Descreva a natureza do tratamento: como serão coletados, utilizados, armazenados e eliminados os dados? Como eles serão coletados? Eles serão compartilhados com quem? Se houver um fluxograma do tratamento, insira-o. Quais tratamentos podem ser considerados de alto risco?

Descreva o escopo do tratamento: qual a categoria dos dados? Qual o volume de dados que serão tratados? Com que frequência? Por quanto tempo? Quantos titulares serão afetados? Há limitação ou previsão por área geográfica?

Descreva o contexto do tratamento: qual é a relação da organização com os titulares? Quanto controles terão? Eles têm uma expectativa de que seus dados serão usados dessa forma? Há dados de crianças ou outro grupo vulnerável? Existe alguma questão peculiar sobre o tratamento ou sua segurança? É inovador de alguma forma? Há algum assunto de interesse público que deva ser levado em consideração? A organização está vinculada a algum código de conduta ou certificação? O tratamento respeita os princípios da proporcionalidade e a necessidade?

Descreva a finalidade do tratamento: o que se pretende alcançar? Qual é o efeito que se terá sobre os titulares? Quais são os benefícios do tratamento para a organização e para a sociedade?

3. Identificação dos riscos à privacidade

Descreva os riscos e o possível impacto nos titulares.	**ID**	**Probabilidade**	**Impacto**	**Grau de risco**
Acesso não autorizado aos documentos físicos armazenados no escritório	#1	3	2	6 (moderado)
...	**#2**	**...**	**...**	**...**

TABELA DE CLASSIFICAÇÃO DE RISCOS

PROBABILIDADE						
	5 - QUASE CERTO	**5**	**10**	**15**	**20**	**25**
	4 - PROVÁVEL	**4**	**8**	**12**	**16**	**20**
	3 - POSSÍVEL	**3**	6	**9**	**12**	**15**
	2 - IMPROVÁVEL	2	**4**	**6**	**8**	**10**
	1 - REMOTO	**1**	**2**	**3**	**4**	**5**
MATRIZ DE RISCO		**1 - INSIGNIFICANTE**	**2- BAIXO**	**3- MODERADO**	**4- ELEVADO**	**5- CRÍTICO**
		IMPACTO				

NÍVEL DE RISCO
Risco Baixo
Risco Médio
Risco Alto
Risco Elevado

CLASSIFICAÇÃO DA PROBABILIDADE POR EVENTO		
CLASSIFICACÃO	**DESCRIÇÃO**	**PESO**
1-Remoto	Menos de uma vez por ano	1
2-Improvável	Uma vez por ano	2
3-Possível	Uma vez por semestre	3
4-Provável	Uma vez por mês	4
5-Quase Certo	Uma vez por semana ou mais	5

CLASSIFICAÇÃO DO IMPACTO POR EVENTO		
CLASSIFICACÃO	**DESCRIÇÃO**	**PESO**
1-Insignificante	Sem danos e prejuízos, perda financeira pequena ou indireta. Acontecimentos que não produzam desconforto aos titulares de dados. Sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares.	1
2-Baixo	Acontecimentos que não produzam desconforto aos titulares de dados. Sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares.	2
3-Moderado	Requer tratamento, indica significativa perda financeira. Impacto relacionado à perda e/ou comprometimento de ativos não críticos e/ou descumprimento de leis ou regulamentações que não comprometem a imagem da Empresa. Acontecimentos que produzam desconforto aos titulares. Sem prejuízos financeiros e sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares.	3
4-Elevado	Grandes danos e prejuízos financeiros diretos, perda de capacidade de operação. Impacto relacionado à perda e/ou descumprimento de leis ou regulamentações que comprometem a imagem da empresa. Acontecimentos que podem produzir	4

	restrição às liberdades civis e aos direitos fundamentais dos titulares.	
5-Crítico	Eventos relevantes que comprometem fortemente o resultado da Empresa e sua estratégia. Eventos deste tipo podem afetar o resultado da Empresa de forma relevante. Acontecimentos que produzam restrição às liberdades civis e aos direitos fundamentais dos titulares.	5

4. Medidas de endereçamento dos riscos

Identificar medidas adicionais a serem tomadas para reduzir ou eliminar os riscos identificados como (médio, alto ou elevado).					
Risco	**Grau de risco**	**Recomendações**	**Efeito**	**Risco residual**	**Comentários**
#1	6	Limitar o acesso, passando-se a trancar a sala e exigir uma assinatura com data e hora de cada acesso por colaboradores	Reduzido	Baixo	Recomendação da ISO 27001 – 9.1.1
#2			Eliminado	Moderado	
#3			Aceito		

É possível, dependendo da complexidade, fazer uma tabela para cada tratamento para endereçar corretamente todas as informações.

5. Observações finais

Item	**Nome e data**	**Observações**
Medidas aprovadas por:	Comitê (se for o caso) ou o nome dos responsáveis	Incluir as ações no plano de implementação, mencionando prazo e responsável

Riscos residuais aprovados por:	...	
Verificação pelo DPO:		
Resumo das orientações pelo DPO:		
Orientação pelo DPO aceita ou recusada por:		Se recusada, explicar as razões.
Comentários:		
Este Relatório de Impacto à Proteção de Dados Pessoais foi aprovado em:	Data	
Este Relatório deverá ser revisado periodicamente por:		