Protocolo: ***816431***
Data: ***02/08/2022***
Título: ***RESOLUÇÃO Nº 91***
Página(s): ***a***

RESOLUÇÃO SEGOVI Nº 91 DE 1º DE AGOSTO DE 2022

Regulamenta o Programa de Governança em Privacidade e Proteção dos Dados Pessoais - PGPPDP no âmbito da Administração Pública Municipal, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

O SECRETÁRIO MUNICIPAL DE GOVERNO E INTEGRIDADE PÚBLICA, no uso das atribuições que lhe são conferidas pela legislação em vigor, e

CONSIDERANDO o disposto no inciso LXXIX, do art. 5º, da Constituição da República Federativa do Brasil de 1988, incluído pela Emenda Constitucional nº 115, de 10 de janeiro de 2022, o qual estabelece que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

CONSIDERANDO o disposto na Lei Federal nº 13.709, Lei Geral de Proteção de Dados Pessoais - LGPD;

CONSIDERANDO o disposto no Decreto Rio nº 49.558, de 06 de outubro de 2021, que *estabelece os procedimentos iniciais a serem adotados pela Administração Pública Municipal visando à construção de uma cultura de proteção de dados pessoais e dá outras providências* , em especial seu art. 3º, parágrafo único, segundo a qual caberá à Secretaria Municipal de Governo e Integridade Pública - SEGOVI propor as medidas de governança necessárias à implementação do Programa de Proteção de Dados no âmbito da PCRJ,

RESOLVE:

Art. 1º Esta Resolução tem por objetivo regulamentar o Programa de Governança em Privacidade e Proteção dos Dados Pessoais - PGPPDP que será implementado pelos agentes de tratamento de dados pessoais no âmbito da Administração Pública Municipal, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

Parágrafo único. A elaboração do PGPPDP seguirá as diretrizes constantes da LGPD e do Decreto Rio nº 49.558, de 06 de outubro de 2021, assim como as Instruções Normativas e as Resoluções publicadas pela Autoridade Nacional de Proteção de Dados, as diretrizes relativas à Governança de Dados e ao Sistema Municipal de Informática, além dos demais regramentos sobre o tema.

Art. 2º Para fins desta Resolução considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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

III - titular dos dados: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento;

IV - agentes de tratamento: o controlador e o operador. Os indivíduos subordinados ou vinculados, como os funcionários, os servidores públicos ou as equipes de trabalho de um órgão ou de uma entidade, que atuam sob o poder diretivo do agente de tratamento não serão considerados como controladores ou operadores;

V - controlador: órgão da Administração Direta ou entidade da Administração Indireta, do Poder Executivo do Município do Rio de Janeiro, a quem compete as principais decisões relativas aos elementos essenciais para o cumprimento da finalidade do tratamento de dados pessoais, bem como a definição da natureza dos dados pessoais tratados e a duração do tratamento;

VI - controladoria conjunta: determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais para a finalidade e instruções previamente estabelecidas pelo controlador. Em sendo pessoa jurídica, os empregados, administradores, sócios, servidores e outras pessoas naturais que a integram e cujos atos expressam a atuação desta, não serão considerados como operadores.

VIII - suboperador: é o contratado pelo operador, após a autorização formal do controlador, para auxiliar no tratamento de dados pessoais em nome do controlador, podendo ser equiparado ao operador perante a LGPD em relação às atividades que foi contratado para executar, no que se refere às responsabilidades.

IX - encarregado: pessoa indicada, mediante ato formal, pelo controlador e pelo operador, cuja identidade e informações de contato estarão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador e do operador, sendo responsável por atuar como canal de comunicação entre o controlador, o operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD;

X - tratamento de dados pessoais: 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;

XI - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, não sendo a única nem a principal base legal possível para viabilizar o tratamento de dados pessoais;

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

XIII - Autoridade Nacional de Proteção de Dados - ANPD: órgão da Administração Pública Federal, cujos papéis e competências estão definidos na Lei Federal nº 13.709, de 14 de agosto de 2018, (Lei Geral de Proteção de Dados - LGPD), entre eles: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

Art. 3º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais - PGPPDP terá sua elaboração e implementação liderada pelos encarregados de dados nomeados pelos órgãos e entidades da Administração Pública Municipal, que serão apoiados pelas diversas áreas, além de terem livre acesso às assessorias e ao nível estratégico dos órgãos e entidades.

Art. 4º Os órgãos e as entidades deverão criar internamente um Comitê de Privacidade e Proteção de Dados Pessoais para oferecer suporte às atividades dos encarregados de dados, que terá, no mínimo, as seguintes atribuições:

I - apoiar o trabalho dos encarregados de dados na implantação do PGPPDP;

II - auxiliar na elaboração dos instrumentos do Programa;

III - fornecer informações acerca dos tratamentos de dados pessoais realizados no âmbito do órgão ou entidade;

IV - tirar dúvidas e prestar esclarecimentos acerca das atividades realizadas pelas suas áreas e demais setores;

V - reavaliar, em conjunto com os responsáveis pelos sistemas, processos de negócio, serviços e políticas públicas, a efetiva necessidade dos tratamentos de dados pessoais realizados;

VI - implementar o Programa em seus órgãos e entidades;

VII - analisar o nível de criticidade em caso de incidente de segurança com dados pessoais e acionar o profissional da tecnologia da informação, se for o caso;

VIII - documentar as respostas aos incidentes relacionados a recursos computacionais ou físicos.

§1º Serão compreendidos, como Comitê de Privacidade e Proteção de Dados Pessoais do órgão ou entidade, o Grupo de Trabalho, o Comitê Multidisciplinar, a Comissão de Proteção de Dados ou demais estruturas semelhantes, desde que possuam atribuições semelhantes àquelas indicadas neste artigo.

§2º O Comitê de Privacidade e Proteção de Dados Pessoais deverá ser coordenado pelo encarregado de dados titular, que terá por atribuição convocar e organizar as reuniões do grupo, além de liderar a elaboração dos instrumentos descritos no artigo 5º desta Resolução.

§ 3º Na hipótese de haver mais de um encarregado de dados titular nomeado para o órgão ou entidade, a coordenação do Comitê de Privacidade e Proteção de Dados Pessoais deverá ser exercida por um dos encarregados de dados, a ser definido pelo Comitê.

§4º O órgão ou entidade deverá publicar por meio de Resolução a composição do seu Comitê de Privacidade e Proteção de Dados Pessoais.

§5º O Comitê de Privacidade e Proteção de Dados Pessoais deverá ter composição adequada à estrutura administrativa do órgão ou entidade e à escala e ao escopo dos tratamentos de dados pessoais realizados.

Art. 5º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais de cada controlador deverá conter os elementos constantes do art. 50, §2º da LGPD e da Política Municipal de Proteção de Dados, devendo ser composto, no mínimo, dos seguintes instrumentos:

I - Termo de Uso;

II - Termo de Consentimento;

III - Inventário de Dados Pessoais;

IV - Orientações do Controlador para o Operador;

V - Plano de Análise de Riscos;

VI - Plano de Adequação;

VII - Aviso de Privacidade e Política de Privacidade;

VIII - Política de Cookies;

IX - Plano de Resposta aos Incidentes de Proteção de Dados Pessoais;

X - Relatório de Incidente de Proteção de Dados Pessoais;

XI - Política de Controle de Acessos;

XII - Relatório de Impacto de Proteção de Dados de Pessoais (RIPD);

XIII - Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos para fins de adequação às leis de proteção de dados pessoais dos órgãos e das entidades; e

XIV - Cronograma de Implementação do PGPPDP.

§1º Para iniciar a implementação do PGPPDP, o encarregado de dados deverá elaborar e publicar, pelo menos, e com o apoio do Comitê de Privacidade e Proteção de Dados Pessoais a que se refere o art. 4º, o cronograma de implementação do Programa.

§2º Após a elaboração dos instrumentos constantes do caput do art. 5º, estes deverão ser validados Secretário ou seu substituto, no caso de Administração Direta, ou o Presidente, Diretor ou substituto, no caso de Administração Indireta.

Art. 6º As orientações e elementos mínimos para elaborar os instrumentos do PGPPDP encontram-se no Anexo II desta Resolução.

Art. 7º Os instrumentos relativos ao PGPPDP deverão ser revistos e atualizados periodicamente, sendo o período mínimo para atualização a cada 12 (doze) meses.

Art. 8º Os órgãos e entidades da Administração Municipal Direta e da Indireta possuem os prazos limites estabelecidos no Anexo I para elaboração e implementação dos instrumentos mencionados no artigo 5º desta Resolução.

Parágrafo único. Os prazos estabelecidos no Anexo I serão contados em dias corridos contados a partir publicação desta Resolução e não isentam os órgãos e entidades de apresentarem os documentos requisitados pela ANPD e órgãos de controle.

Art. 9º Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro,1º de agosto de 2022.

TONY CHALITA
Secretário Municipal de Governo e Integridade Pública

Anexo I - Prazos Limites

Prazos limites para elaboração e implementação dos instrumentos do PGPPDP, contados a partir da publicação da Resolução	
Termo de Uso	Até 90 dias
Termo de Consentimento (quando o consentimento for a base legal cabível)	Até 90 dias
Inventário de Dados Pessoais	Até 240 dias
Orientações do Controlador para o Operador	Até 60 dias
Plano de Análise de Riscos	Até 270 dias
Plano de Adequação	Até 270 dias
Aviso de Privacidade e Política de Privacidade	Até 90 dias
Política de Cookies	Até 90 dias
Plano de Resposta aos Incidentes de Proteção de Dados Pessoais	Até 300 dias

Relatório de Incidente de Proteção de Dados Pessoais	Até 150 dias
Política de Controle de Acessos	Até 120 dias
Relatório de Impacto de Proteção de Dados de Pessoais (RIPD)	Até 300 dias
Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos para fins de adequação às leis de proteção de dados pessoais dos órgãos e das entidades	Até 60 dias

Anexo II - Descrição dos Elementos Mínimos dos Instrumentos do Programa de Governança em Privacidade e Proteção dos Dados Pessoais (PGPPDP)

I - Termo de Uso

1. O Termo de Uso é o documento que estabelece as regras e as condições de uso em que ocorrem os tratamentos de dados do órgão ou entidade da Administração Pública Municipal, devendo permitir a publicização das atividades, e suas finalidades específicas, realizadas quando houver tratamento de dados pessoais, especialmente (mas não limitado a) para a execução de políticas públicas, em cumprimento ao art. 23, inciso I, da LGPD.

2. O agente de tratamento de dados pessoais deve se pautar pela obrigação de transparência com o titular de dados, devendo o Termo de Uso informar como as atividades de tratamento de dados atendem às obrigações constantes na LGPD, principalmente aos direitos do titular constantes do art. 9º e do art. 18.

3. O Termo de Uso deve conter, no mínimo, os seguintes elementos:

I - Identificar quais os tratamentos de dados pessoais são realizados pelo controlador, e suas bases legais;

II - Na hipótese de a base legal ser execução de políticas públicas pelo controlador, deve ser destacado o regramento legal em que consta a política pública e a finalidade específica do uso dos dados pessoais, destacando-se a real necessidade de utilização daquele dado para a política pública executada;

III - Identificar eventuais contratos, convênios e termos de cooperação que servem de subsídio para a execução descentralizada da política pública;

IV - Identificar as atribuições dos órgãos ou entidades constantes do SICI ou do regimento interno ou ainda da sua lei de criação que justificam a execução, pelo órgão ou entidade, daquela finalidade pública;

V - Identificar quais compartilhamentos de dados pessoais são realizados, com quais instituições e quais os regramentos (leis, decretos, portarias, resoluções, convênios, Acordos) que fundamentam tal compartilhamento;

VI - Informar a dispensa do consentimento, na hipótese de tratamento de dados pessoais sensíveis, conforme art. 11, II, b, da LGPD;

VII - Informar o ciclo de vida dos dados;

VIII - Informar os direitos do titular dos dados pessoais;

IX - Informar responsabilidades do usuário e da Administração Pública;

X - Outros requisitos que possam auxiliar no cumprimento das disposições da LGPD, principalmente a garantia dos direitos do titular de dados.

4. Os órgãos e entidades devem tornar o Termo de Uso disponível publicamente no seu sítio eletrônico, atualizando com a periodicidade mínima prevista no art. 7º desta Resolução, havendo a necessidade de publicar no sítio eletrônico do órgão ou entidade, de preferência com a indicação e demonstração de todas as versões do documento.

II - Termo de Consentimento

5. O Termo de Consentimento é o documento pelo qual o titular dos dados formaliza o consentimento fornecido ao controlador ou operador quando a base legal de tratamento for aquela constante do art. 7º, I, da LGPD.

6. O consentimento é a manifestação livre, informada, inequívoca e, para o caso do tratamento na hipótese do art. 11, I, da LGPD, de forma específica e destacada, pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade determinada.

7. O Termo de Consentimento deve ser redigido de maneira clara, objetiva e, sempre que possível, baseado em linguagem simples, de modo a facilitar a compreensão do titular dos dados.

III - Inventário de Dados Pessoais

8. 8. O Inventário de Dados Pessoais é o documento que consiste no registro interno das operações de tratamento dos dados pessoais realizados pelos órgãos e entidades da Administração Pública Municipal, em cumprimento ao art. 37 da LGPD.

9. O Inventário de Dados Pessoais deve conter, no mínimo, os seguintes elementos:

I - A identificação do processo de negócio/serviço;

II - Os ativos que serão utilizados para fazer o tratamento de dados;

III - Finalidade do tratamento (o que a instituição faz com o dado pessoal);

IV - Atores envolvidos;

V - Dados pessoais e dados pessoais sensíveis utilizados;

VI - Categoria dos titulares dos dados pessoais;

VII - Origem dos dados;

VIII - Localização e forma de armazenamento;

IX - Base legal de tratamento (art. 7º, 11 e 14 da LGPD);

X - Previsão legal

XI - Ciclo de vida dos dados pessoais;

XII - Compartilhamentos com terceiros;

XIII - Transferência internacional de dados (art. 33 LGPD); e

XIV - Medidas de segurança da informação atualmente adotadas.

10. O inventário de dados pessoais deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no inventário.

11. O inventário de dados pessoais deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados e é realizado pelo órgão ou entidade, devendo ser o mais completo e detalhado possível, atualizado com periodicidade mínima de 12 (doze) meses e servir como subsídio para a elaboração do Plano de Análise de Riscos, entre outros instrumentos da Governança em Privacidade e Proteção de Dados Pessoais.

IV - Orientações do Controlador para o Operador

12. As Orientações do Controlador para o Operador devem estar contidas em um documento que estabelece as regras para a execução do tratamento de dados pessoais pelos Operadores, em cumprimento ao art. 39, da LGPD.

13. Os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres devem prever como um dos seus anexos o documento que contém as orientações específicas para tratamento de dados pessoais fornecidas pelo controlador ao operador.

14. Caso os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres não possuam cláusula específica e destacada acerca do tratamento de dados pessoais, devem ser aditados para conter tais cláusulas e para conter as Orientações do Controlador para o Operador.

15. As Orientações do Controlador para o Operador devem conter, no mínimo, os elementos decisórios principais, entre os quais destacam-se a finalidade do tratamento, estipulando os objetivos que justificam a realização do tratamento, a natureza dos dados pessoais tratados, a duração do tratamento, incluindo o estabelecimento de prazo para a eliminação dos dados, entre outros elementos que podem ser considerados essenciais a depender do contexto e das peculiaridades do caso concreto.

V - Plano de Análise de Riscos

16. O Plano de Análise de Riscos é o documento que sistematiza a identificação dos riscos incidentes no tratamento de dados pessoais que podem vir a gerar risco às liberdades civis e aos direitos dos titulares de dados, de forma a subsidiar a elaboração do RIPD, em cumprimento ao artigos 5º, XVII, e 38, parágrafo único, da LGPD.

O Plano de Análise de Riscos deve conter, no mínimo, os seguintes elementos:

I - Descrição do risco;

II - Fundamentação do risco;

III - Classificação do risco;

IV - Ações para mitigação do risco;

V - Definição do risco residual esperado após a realização das ações de mitigação dos riscos;

VI - Etapa de monitoramento do risco residual; e

VII - Procedimento de comunicação de quaisquer alterações incidentes sobre o(s) risco(s) e/ou os controles instituídos.

17. O Plano de Análise de Risco deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo os novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no Plano.

18. O Plano de Análise de Risco deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados é realizado pelo órgão ou entidade, devendo ser o mais completo e detalhado possível, devendo ser atualizado com periodicidade mínima de 12 (doze) meses.

19. O Plano de Análise de Risco contemplará apenas os riscos ao cumprimento das legislações e melhores práticas de proteção de dados pessoais, não sendo considerados todos os possíveis riscos de segurança da informação incidentes, que serão objeto de regulamentação específica.

VI - Plano de Adequação

20. Plano de Adequação é o documento que contém as diretrizes gerais para uma boa governança e alinhamento às práticas da LGPD, estabelecendo as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, em cumprimento ao artigo 50 da LGPD.

21. O Plano de Adequação deve conter, no mínimo, os seguintes elementos:

I - Identificar quais as tecnologias, processos e mudanças organizacionais que precisam ser implementadas para garantir o atendimento aos direitos dos titulares de dados pessoais e aos princípios constantes na LGPD;

II - Descrever de que modo serão implementadas as ações de mitigação dos riscos identificados no Plano de Análise de Riscos;

III - Apontar de que forma as medidas de segurança da informação apontadas no Inventário de Dados Pessoais precisam ser aperfeiçoadas e atualizadas para que sejam adotados os controles de segurança adequados para o tratamento dos dados;

IV - Elaborar um cronograma de implementação das medidas identificadas como necessárias à adequação;

V - Adequar os processos de trabalho, serviços e políticas públicas seguindo boas práticas de minimização de dados pessoais, privacidade por padrão e privacidade desde a concepção (*privacy by design*);

VI - Oferecer elementos para suportar a elaboração do Relatório de Impacto a Proteção de Dados Pessoais (RIPD);

VII - Estabelecer processo de comunicação com a ANPD e com o titular de dados na hipótese de ocorrência de incidentes de proteção de dados pessoais ou vazamento de dados pessoais;

VIII - Indicar de que modo será dada publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nos sítios eletrônicos dos órgãos e das entidades;

IX - Indicar de que modo serão atendidas as exigências que vierem a ser estabelecidas pela ANPD, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da LGPD; e

X - Desenvolver plano de capacitação sobre privacidade e proteção de dados pessoais para os agentes públicos dos órgãos e das entidades municipais.

22. Os órgãos e entidades deverão tornar o seu Plano de Adequação acessível a todos os funcionários da sua instituição, devendo ser feitos esforços no sentido de capacitar e sensibilizar os agentes públicos do órgão ou entidade para a necessidade de realizar as adequações necessárias.

23. O Plano de Adequação deverá ser atualizado com periodicidade mínima de 12 (doze) meses.

VII - Política de Privacidade e Aviso de Privacidade

24. A Política de Privacidade é o documento interno pelo qual o controlador informa aos seus agentes públicos a forma como realiza os tratamentos de dados pessoais de um dado serviço ou aplicação ou banco de dados, sendo um documento para uso interno do órgão ou entidade.

25. Aviso de Privacidade é o documento externo pelo qual o controlador transparece ao usuário do serviço ou da aplicação ou do banco de dados a forma como realiza os tratamentos de dados pessoais, e como o Poder Público fornecerá privacidade ao usuário, em cumprimento ao art, 23, I, da LGPD, explicitando, ainda, de que modo são garantidos os direitos do titular constantes do art. 9º e 18.

26. O Aviso de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores (se cabível);

III - Identificação dos Encarregados;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade; e

VIII - Tratamento posterior dos dados para outras finalidades.

27. A Política de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores;

III - Identificação dos Encarregados;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade;

VIII - Regras de segurança da informação dos dados pessoais;

IX - Tratamento posterior dos dados para outras finalidades; e

X - Transferência internacional de dados.

28. Os órgãos e entidades devem tornar o Aviso de Privacidade disponível publicamente no seu sítio eletrônico, atualizando com a periodicidade mínima prevista no art. 7º desta Resolução, sendo desnecessária a publicação da Política de Privacidade.

VIII - Política de Cookies

29. A Política de Cookies é o documento informativo pelo qual o usuário deverá ser informado sobre quais dados são coletados e armazenados ao navegar por uma das páginas de titularidade do Poder Público Municipal, e para qual funcionalidade, além de quais medidas de segurança são

implementadas em seu uso.

30. A Política de Cookies deve conter, no mínimo, os seguintes elementos:

I - Quais cookies são utilizados (cookies proprietários e de terceiros);

II - Quais os dados são coletados pelos cookies;

III - Qual a finalidade do uso de cookies;

IV - Como o usuário pode obter mais informações sobre os cookies de terceiros utilizados no serviço.

31. Além da elaboração da Política de Cookies, cujo auxílio especializado será de competência da IplanRio, deve ser disponibilizado no site do órgão ou entidade um banner ou aviso para dar ciência ao usuário, com o mapeamento e discriminação dos cookies, permitindo que o usuário possa fazer escolhas e possa definir, sistemicamente, o que acontece quando se recusa um ou outro grupo.

32. O banner ou aviso para dar ciência ao usuário deve ser redigido preferencialmente em português.

33. Os órgãos e entidades deverão tornar a Política de Cookies disponível publicamente nos seus sítios eletrônicos.

IX - Plano de Resposta aos Incidentes de Proteção de Dados Pessoais

34. O Plano de Resposta aos Incidentes de Proteção de Dados Pessoais é o documento que estabelece quais protocolos deverão ser seguidos em caso de ocorrência de incidentes, em atendimento ao art. 50, § 2º, II, g, da LGPD.

35. O Plano de Resposta deverá estabelecer quais as medidas de resposta para a hipótese de ocorrência dos riscos contidos no Plano de Análise de Riscos, estabelecendo medidas de curto, médio e longo prazos, recursos disponibilizados para a resposta, atores responsáveis e de que modo serão remediados os danos causados pelos incidentes.

36. Todos os agentes públicos dos órgãos e das entidades que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas no Plano de Resposta.

X - Relatório de Incidente de Proteção de Dados Pessoais

37. O Relatório de Incidentes de Proteção de Dados Pessoais é o documento que informa detalhadamente sobre o incidente que ocorreu, e de que modo a comunicação deverá ser feita, em atendimento ao art. 50, § 2º , II, g, da LGPD.

38. O Relatório de Incidentes deverá comunicar detalhadamente o incidente, que deverá ser feita em prazo razoável, conforme definido pela ANPD, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

39. O encarregado de dados do órgão ou entidade deve elaborar o Relatório, que deve ser validado pelo titular da pasta previamente ao envio à ANPD.

40. O Relatório em sua versão final deve ser tornado público, devendo ser excluídas as informações sobre os titulares envolvidos.

XI - Política de Controle de Acessos

41. A Política de Controle de Acesso tem como objetivo, habilitar o acesso de serviços e de sistemas de responsabilidade dos órgãos e das entidades, apenas aos órgãos/entidades/usuários devidamente autorizados.

42. A Política de Controle de acesso deverá, no mínimo:

I - definir claramente as responsabilidades/papéis dos intervenientes desse processo;

II - atender ao princípio do menor privilégio; e

III - possuir perfis de acesso bem definidos e regras claras para habilitação, suspensão e revogação de direitos de acesso e que trate:

a) o controle de acesso aos registros de eventos (logs);

b) o controle de acesso às configurações dos sistemas (perfis administrativos);

c) o controle de acesso às cópias de segurança;

d) o controle de acesso às informações sensíveis e situações que requeiram a propriedade do não-repúdio e o acesso via certificado digital; e

e) os processos formais para a solicitação de acesso aos perfis dos sistemas, permitindo verificar, inclusive, os autorizadores que concederam as permissões ao usuário.

43. Os órgãos e entidades devem realizar periodicamente a revisão dos direitos de acesso e da sua Política de Controle de Acesso.

44. Todos os agentes públicos dos órgãos e das entidades que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas na Política de Controle de Acesso.

XII - Relatório de Impacto de Proteção de Dados de Pessoais (RIPD)

45. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o documento 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, em atendimento ao art. 5º, inciso XVII, da LGPD.

46. O RIPD deverá conter elementos e informações de todos os instrumentos constantes desta Resolução, além de informações adicionais que o encarregado de dados julgar pertinentes.

47. A ANPD poderá solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

48. A elaboração do Relatório de Impacto à Proteção de Dados Pessoais deverá seguir as orientações e metodologia divulgadas pela ANPD.

XIII - Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos para fins de adequação às leis de proteção de dados pessoais dos órgãos e das entidades

49. O controlador deverá identificar os seus contratos, convênios, Termos de Cooperação, Acordos de Resultados, editais de licitação e demais documentos jurídicos congêneres em que se realize o tratamento ou o compartilhamento de dados pessoais e que possam precisar de futuras

modificações para serem adequados à LGPD.

50. O Comitê de Privacidade criado para apoiar a atuação dos encarregados de dados do órgão ou entidade deverá elaborar um cronograma para identificar e mapear os instrumentos jurídicos para fins de adequação às leis de proteção de dados pessoais.

XIV - Cronograma de Implementação do PGPPDP

51. Os órgãos e entidades deverão elaborar um cronograma de implementação dos instrumentos do PGPPDP, que demonstrará o comprometimento do agente de tratamento de dados em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme art. 50, §2º, inciso I, alínea "a".

52. O cronograma de implementação deverá conter as etapas de elaboração dos instrumentos, informando, sempre que possível, prazos e responsáveis, cabendo revisão dos prazos, desde que justificada.

53. O cronograma de implementação deve ser tornado público no site do órgão ou entidade.