RELATÓRIO DE DESENVOLVIMENTO DO ESTUDO DE IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/18 - NO TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO

Tribunal de Contas DO MUNICÍPIO DE SÃO PAULO

Sumário

1. Considerações sobre o produto final almejado pelo projeto 3
2. Reuniões do Grupo 5
3. Estudo e debate sobre os conceitos fundamentais da LGPD 6
4. Coleta de Informações em outros tribunais e órgãos públicos 10
4.1. Nota técnica nº 01/19 do Instituto Rui Barbosa. 10
4.2. Experiência do TCU. 19
4.3. Experiência de outros Tribunais de Contas. 21
4.4 Relatório do Grupo de Estudo da Prefeitura Municipal de São Paulo 23
4.5. Site do Tribunal de Justiça do Estado de São Paulo. 24
5. Normativos do TCMSP que podem ser impactados pela implantação da LGPD. 26
6. Mapeamento das áreas do TCM - *Data Flow Map* 28
6.1 Informações obtidas pela aplicação de formulário 29
6.2 Reflexões sobre as informações obtidas 43
6.2.1 Conceitos 43
6.2.2. Acesso e Utilização 44
6.2.3 Tempo e Armazenamento 45
6.2.4. Tratamento 47
6.3 Conclusões 48
7. *Data protection by design* (Privacidade por definição) 54
8. Escolha da estrutura funcional 55
9. Constatações inerentes à Tecnologia da Informação 60
10. Providências urgentes a serem adotadas pelo TCMSP em decorrência do início da vigência da LGPD 68
11. Demais providências a serem adotadas 71
12. Dúvidas e Circunstâncias 72

1. Considerações sobre o produto final almejado pelo projeto

O projeto, que faz parte do *Plano Anual 2020* da Assessoria Jurídica de Controle Externo, prevê, como produto final, inserido na declaração de escopo, a *elaboração de manual de boas práticas, ou instrumento análogo, para o tratamento de dados pessoais no âmbito deste TCMSP, a partir dos trabalhos desenvolvidos por um Grupo de Estudos para avaliar os impactos da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) - no Tribunal de Contas do Município de São Paulo*.

Não obstante, depois de muitas *idas e vinda*s relacionadas à vigência da lei, decorrentes da edição da Medida Provisória nº 959/2020[1], o Senado Federal, ao tratar do projeto de conversão da referida MP em lei, deliberou que a matéria inerente à entrada em vigor da LGPD estaria preclusa.

Com isso, a LGPD passou a vigorar aos **18.09.2020**, após a sanção, pelo Presidente da República, da Lei Federal 14.058/2020[2].

Nesse contexto, a atuação do Grupo de Estudos passou a tomar contornos mais abrangentes, para o fim de delinear as **providências para o início imediato da implantação da LGPD** no âmbito desta Colenda Corte.

[1] Que prorrogou a vigência da lei para 31.12.2020.
[2] Originada da Medida Provisória nº 959/20 que, apesar de tratar da operacionalização do Benefício Emergencial pago a trabalhadores com redução de jornada e suspensão de contrato durante a pandemia do coronavírus, também continha matéria inerente à entrada em vigor da LGPD.

Cumpre anotar que, aos 16.09.2020, foi publicado no D.O.C. o Decreto Municipal nº 59.767/2020[3], que regulamenta a aplicação da LGPD no âmbito da Administração Municipal direta e indireta.

A normatização municipal apresenta três pontos fundamentais: (i) a definição dos conceitos utilizados e os princípios que delimitam as atividades de tratamento, retirados da lei e adequados à realidade municipal; (ii) a atribuição de responsabilidades para a Administração Pública Municipal Direta e Indireta, com respeito, no caso das entidades da Administração Pública Indireta, da autonomia e dos limites do poder de tutela; e (iii) a forma e os requisitos para o tratamento de dados pessoais pela Administração Pública Municipal.

Apresenta, ainda, três funções essenciais: (i) mapeamento de dados (medida de identificação dos procedimentos internos utilizados para o tratamento dos dados pessoais no âmbito da Prefeitura de São Paulo, e dos riscos no tratamento dos dados em cada órgão público, possibilitando a aplicação de soluções condizentes com a política municipal de proteção de dados e da privacidade); (ii) análise da LAI (Lei de Acesso à Informação) – LGPD (medida realizada pela Comissão Municipal de Acesso à Informação, colegiado plúrimo, dotado de legitimidade e competente para deliberações sobre a aplicação da LAI, deverá ser responsável pela deliberação de: (i) proposta de diretrizes para elaboração dos planos de adequação; e (ii) qualquer assunto relacionado à aplicação da Lei Geral de Proteção de Dados Pessoais e de seu respectivo decreto regulamentador); e (iii) fica designado o Controlador Geral do Município como o encarregado da proteção de dados pessoais.

[3] http://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020

Assim, a elaboração deste relatório se tornou indispensável para **dar conhecimento sobre os trabalhos realizados**, bem como para **enumerar as providências emergenciais a serem adotadas no processo de implantação da legislação no âmbito do TCMSP**.

2. Reuniões do Grupo

Aos 06 de março de 2020 ocorreu, nas dependências do Tribunal, a primeira reunião do grupo com apresentação do projeto. A partir desta data, com o início do *home office*, as reuniões foram feitas virtualmente[4]:

1ª reunião virtual	30/03/2020	Estudo e debate sobre os conceitos fundamentais da LGPD.
2ª reunião virtual	28/04/2020	Distribuição de tarefas: mapeamento das áreas.
3ª reunião virtual	10/06/2020	Operacionalização para o encaminhamento do questionário para as áreas do TCM.
4ª reunião virtual	02/07/2020	Operacionalização para o encaminhamento do questionário para as áreas do TCM.
5ª reunião virtual	15/07/2020	Elaboração de questões a serem formuladas no evento programado para o dia 16.07.
6ª reunião virtual	16/07/2020	Participação na Webinar: "Desafios na Implantação da LGPD" (via Escola de Gestão e Contas do TCMSP). Palestrantes: Fernando Santiago, Andrea Willemin e Carlos Alberto S. Freitas (TCU).
7ª reunião virtual	19/08/2020	Apresentação do relatório de desenvolvimento.
8ª reunião virtual	27/08/2020	Discussão sobre o relatório de desenvolvimento e sobre o resultado do mapeamento.
9ª reunião virtual	03/09/2020	Discussão sobre o relatório de desenvolvimento e sobre o resultado do mapeamento.

[4] Além disso, foi criado grupo de *WhatsApp* que constantemente é alimentado com notícias e informações para facilitar a comunicação dos integrantes.

3. Estudo e debate sobre os conceitos fundamentais da LGPD

Em breve síntese, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, dispõe sobre o tratamento de dados pessoais, nos meios digitais ou físicos, inclusive por pessoa jurídica de direito público.

A legislação foi redigida com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, estabelecendo regras e limites para empresas e organizações a respeito da coleta, armazenamento, tratamento e compartilhamento de dados.

Possui, ainda, a finalidade de criação de um ambiente de segurança jurídica para o armazenamento dos dados.

Dentre os principais conceitos trazidos na LGPD, também trazidos no bojo do Decreto Municipal nº 59.767/2020[5], destacam-se:

[5] Art. 2º *Para os fins deste decreto, 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 - *dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*;
IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais em suporte eletrônico ou físico;
V - *titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*;
VI - *controlador: pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*;
VII - *operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador*;
VIII - *encarregado: pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)*;

Art. 5º *Para os fins desta Lei, 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*;

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

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

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

X - *tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*.

IX - *agentes de tratamento: o controlador e o operador*;
X - *tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*;
XI - *anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*;
XII - *consentimento: manifestação livre, informada e inequívoca pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para uma finalidade determinada*;
XIII - *plano de adequação: conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais.*

Ademais, todas as regras descritas pelos arts. 23 a 30 da LGPD devem ser observadas pelos órgãos e entidades públicas.

Daquilo que nos importa, fazem-se as seguintes transcrições da LGPD:

> Art. 23. *O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado 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*:
>
> I - *sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos*;
>
> III - *seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei*;
>
> § 1º *A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento*.
>
> § 2º *O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)*.
>
> § 3º *Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)*.
>
> (...)

Art. 25. *Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral*.

Art. 26. *O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei*.

§ 1º *É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto*:

I - *em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)*;

III - *nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei*.

IV - *quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres*;

V - *na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados*; ou

IV - *quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres*;

V - *na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades*.

§ 2º *Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional*.

Art. 27. *A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto*:

I - *nas hipóteses de dispensa de consentimento previstas nesta Lei*;

> II - *nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei*; ou
>
> III - *nas exceções constantes do § 1º do art. 26 desta Lei*.

4. Coleta de Informações em outros tribunais e órgãos públicos

4.1. Nota técnica nº 01/19 do Instituto Rui Barbosa.

O Instituto Rui Barbosa disponibilizou a Nota Técnica nº 01/19 (documento anexo - doc. 01) para tratar da LGPD no âmbito dos Tribunais de Contas.

Anota-se, ainda, que, em consulta ao sítio eletrônico da Atricon consta a referência à elaboração do respectivo documento do IRB, reforçando sua utilidade no processo de tratamento de dados a ser operacionalizado pelos Tribunais.

Destacam-se do texto da referida Nota Técnica os seguintes pontos:

► Sobre os pré-requisitos estruturantes:

> *O uso da tecnologia da informação e das técnicas de tratamento de dados tem sido cada vez mais explorado pelos Tribunais de Contas como instrumento para o exercício de suas funções legais e constitucionais de forma mais efetiva e eficiente.*
> *Nesse contexto, os deveres de transparência e de acesso à informação proativa, associado ao regime jurídico existente sobre direito à*

privacidade, já exigiam dos órgãos públicos uma série de medidas de controle e de auto-organização.
Frente a isso, investir em temas relacionados à gestão de processos, gestão de riscos, segurança da informação e classificação da informação mostra-se ainda mais relevante com o advento da LGPD.

► Sobre a gestão de processos:

A Gestão de Processos engloba o estudo do trabalho, que é o processo de observação e levantamento de informações de um fenômeno, objetivando detalhar sua lógica de funcionamento. A partir disso, busca-se o entendimento do trabalho para compreender suas particularidades e entender sua lógica de existência.
Partindo da premissa de que as necessidades são muitas e os recursos são escassos, as organizações públicas, entre as quais os Tribunais de Contas, devem priorizar ações e otimizar recursos para alcançar melhores resultados. A readequação da estrutura administrativa e a redução do gasto público são desafios importantes à manutenção dos serviços públicos.
Para enfrentar esses desafios, é necessário valer-se de modelos de governança corporativa mais eficientes. Nesse sentido, as constantes inovações tecnológicas, somadas à intensificação do uso de Big Data nas organizações do mundo todo, trouxeram uma nova roupagem ao gerenciamento dos negócios, marcando a transformação dos modelos de governança corporativa.

► Sobre a gestão de riscos:

Para atender ao disposto na LGPD, é necessário que os Tribunais de Contas, enquanto controladores de dados, tenham conhecimento dos riscos que podem ser gerados às liberdades civis e aos direitos fundamentais quando realizarem processos de tratamento de dados pessoais.
(...)
Segundo o Manual de Gestão de Riscos do TCU (BRASIL, 2018, p.18), a Gestão de Riscos tem como um dos seus princípios a aplicação de forma contínua e integrada aos processos de trabalho de uma instituição. Esses processos de trabalho, quando devidamente

mapeados, geram as informações necessárias para subsidiar as seguintes etapas:

- *Estabelecimento do contexto;*
- *Identificação dos riscos;*
- *Análise dos riscos;*
- *Avaliação dos riscos;*
- *Tratamento dos riscos;*
- *Comunicação e consulta com partes interessadas;*
- *Monitoramento;*
- *Melhoria contínua.*

Os dois elementos constituintes das fontes de risco são: a ameaça e a vulnerabilidade. Ambos potencializam as chances de um evento afetar, negativamente, o alcance dos objetivos estratégicos de uma organização.

Num outro aspecto, a Gestão de Riscos revela a necessidade de identificar os níveis de risco: impacto e probabilidade que uma determinada atividade ou um conjunto de atividades (processo) podem afetar, negativamente, o alcance dos objetivos estratégicos da instituição. Aqui, mais uma vez, cabe lembrar que o mapeamento prévio dos Fluxos de Processo possibilita uma gestão proativa na mitigação de riscos.

Quando implementada e mantida segundo a ISO 31000:2009, a gestão dos riscos possibilita a uma organização:

- *Melhorar a efetividade operacional;*
- *Aumentar a probabilidade de atingir os objetivos;*
- *Encorajar uma gestão proativa;*
- *Melhorar a identificação de oportunidades e ameaças;*
- *Melhorar a governança;*
- *Melhorar os controles.*

Nesse contexto, a implantação adequada da LGPD exigirá que os Tribunais de Contas atentem para a gestão eficaz dos riscos relacionados à proteção dos dados pessoais, não apenas nas atividades do controle externo, mas na instituição como um todo.

► Sobre segurança da informação[6]:

[6] A Nota Técnica descreve os 5 (cinco) pilares que sustentarão a prática dessa política pela instituição.

A LGPD exige que as organizações implementem medidas técnicas e administrativas apropriadas para garantir que os dados pessoais sejam processados de forma segura.

► Sobre classificação da informação:

A classificação da informação, nas suas várias abordagens, pode ser considerada uma das boas práticas para governança de dados".
(...)
De acordo com a cartilha sobre classificação da informação editada pelo Tribunal de Contas da União (BRASIL, 2010), as informações são classificadas conforme a:
-confidencialidade: garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas em algum local ou transmitidas por meio de redes de comunicação;
-disponibilidade: garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período definido pelos gestores da informação;
-integridade: garantir a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital. Evitar que a informação seja apagada ou alterada de qualquer forma sem a permissão do gestor.
(...)
Uma vez realizada essa classificação, os Tribunais de Contas terão condições de envidar esforços adequados, necessários e proporcionais aos níveis de proteção exigidos, resultando, assim, no uso racional dos recursos (controles) utilizados.

► Sobre o tratamento de dados pessoais nas atividades administrativas:

(...) a Lei Federal nº 13.460/2017 – que dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos na administração pública – previu como diretriz a necessidade de aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao usuário e a propiciar melhores condições para o compartilhamento das informações (artigo 5º, inciso XIII).

São exemplos disso o uso de redes sociais, os portais de transparência, os cursos ministrados pelas Escolas de Contas, os Serviços de Informação ao Cidadão (SIC), os canais de comunicação do tipo "Fale Conosco" e "Ouvidoria", a emissão de certidões, entre outros. Nesses casos, é bastante provável que ocorra a coleta e o armazenamento de informações pessoais de usuários.

Ademais, no desempenho de suas funções administrativas, as Cortes de Contas recebem, arquivam e compartilham diversos dados pessoais, como na contratação de terceirizados e de serviços autônomos, no cadastro de visitantes, na realização de um concurso público (dados dos candidatos inscritos), nos registros de servidores (informações como telefone pessoal, endereço residencial, existência de pagamento de pensão, crédito consignado), etc.

(...)

É recomendável, diante disso, a criação de uma comissão ou grupo de trabalho multidisciplinar, com abordagem holística, para fazer o diagnóstico dos impactos, bem como o inventário e o mapeamento dos dados pessoais que trafegam na instituição, identificando os processos de trabalho nos quais são coletados e os documentos em que são inseridos.

Nesse aspecto, cabe referir que a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais (artigo 32), o que já justificaria a adoção de tais ações.

(...)

Assim, as seguintes providências podem ser utilizadas como ponto de partida:

- *implantar ou melhorar a governança de dados;*
- *definir um encarregado;*
- *instituir a gestão de riscos e incidentes de segurança;*
- *fortalecer a segurança corporativa da informação;*
- *institucionalizar um programa ou uma política de governança em privacidade;*
- *revisar os contratos e convênios, inserindo cláusulas de observância à LGPD;*
- *promover capacitação, sensibilização e campanhas para servidores, contratados, jurisdicionados e parceiros sobre os cuidados necessários com o tratamento dos dados pessoais.*

► Sobre a estrutura funcional:

A LGPD prevê, para a gestão do tratamento de dados pessoais, três importantes figuras:
Art. 5º Para os fins desta Lei, considera-se:
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2018)
IX - agentes de tratamento: o controlador e o operador.
(...)
...tem-se que os Tribunais de Contas necessitarão adequar sua estrutura para atender ao que prevê a LGPD no que tange às atribuições das figuras do controlador, do operador e do encarregado (artigos 37 a 41).
Poderão, ainda, se valer das estruturas de comunicação já existentes em suas organizações (a exemplo da Ouvidoria, dos Serviços de Informação ao Cidadão e do Protocolo), desde que permitam aos titulares de dados exercerem seus direitos (artigos 17 e 18 da LGPD) de forma facilitada e gratuita (artigo 6º, inciso IV).
Nesse contexto, ganha sentido a previsão da LGPD, ao sugerir, aos controladores e operadores, 'formular regras de boas práticas e de governança que estabeleçam 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' (artigo 50 da LGPD).

► Sobre o tratamento de dados pessoais no exercício do controle externo:

(...) o tratamento de dados pessoais, quando no atendimento da finalidade pública, na persecução do interesse público e com o

objetivo de executar as competências legais, foi disciplinado pelo artigo 23 da LGPD.

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado 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:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II. - (VETADO) e;

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;

IV. - (VETADO)

Como se percebe, há requisitos específicos previstos na LGPD quando o tratamento de dados pessoais for realizado pelo setor público, o que ocorre pelo fato de a Administração Pública estar envolta em suas atividades por princípios e interesses gerais e coletivos que se sobrepõem aos privados.

Por esse motivo, igualmente, a LGPD não previu, nesses casos, a necessidade de prévio consentimento para o tratamento e compartilhamento dos dados pessoais.

(...)

A previsão do inciso I do artigo 23 exige que os Tribunais de Contas passem a informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais. Além disso, as Cortes deverão fornecer informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

A leitura dessa previsão deve pautar-se pela razoabilidade e adequação, a fim de que a divulgação de tais informações não prejudique nem comprometa as atividades de fiscalização. No entanto, o seu cumprimento exigirá organização e autoconhecimento das Cortes de Contas, que deverão ter o devido domínio de seus bancos de dados.

(...)

Ainda que não exista regulamentação específica dispondo sobre como (e se) os Tribunais de Contas deverão atender de forma ativa ao inciso I do artigo 23, o direito dos titulares de obter tais informações, sob demanda, está expressamente previsto. Para tanto, as Cortes poderão se valer das estruturas de comunicação já existentes em suas organizações (a exemplo da Ouvidoria, dos Serviços de Informação ao Cidadão e do Protocolo), desde que permitam aos titulares de dados exercerem seus direitos de forma facilitada e gratuita.

Por sua vez, o inciso III do artigo 23 prevê que as pessoas jurídicas de direito público deverão indicar um encarregado quando realizarem operações de tratamento de dados pessoais. Conforme explicitado no tópico 3.2, a figura do encarregado é conceituada pelo artigo 5º da LGPD, e suas atividades estão disciplinadas no artigo 41 do mesmo diploma, cabendo, assim, a cada Tribunal de Contas, enquanto no papel de controlador, indicar que pessoa exercerá tais atribuições.

Na divulgação das informações relativas ao exercício do controle externo (a exemplo da publicação ativa de relatórios de auditoria, lista de gestores que tiveram contas julgadas irregulares ou parecer prévio desfavorável, lista de devedores de condenações fixadas pelas Cortes, etc), deve-se levar em consideração os princípios constitucionais, a Lei de Acesso à Informação e a própria previsão expressa no artigo 7º, §324, da LGPD. Isso porque as informações constantes e resultantes dos processos de fiscalização são indiscutivelmente de interesse geral e coletivo (artigo 8º da LAI), sendo que há alto grau de relevância pública em disseminá-las para a sociedade. Tal divulgação concretiza o cumprimento ao princípio da publicidade, fomenta a participação popular e o controle social, e demonstra que os agentes públicos estão cumprindo com seu dever de prestar contas.

► Sobre a LGPD e o compartilhamento de informações:

Quanto à estrutura dos dados, a LGPD prevê:

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à

descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

É preciso também considerar a abrangência da atuação contemporânea dos Tribunais de Contas, em que dados e informações de diversas fontes e origens, públicas ou privadas, podem ser utilizados como insumo para o cumprimento eficiente e efetivo das suas funções.

Ademais, dado o crescente número de políticas públicas multissetoriais e transversais que envolvem diversos entes da federação para a sua execução (transferências voluntárias, por exemplo), mostra-se essencial a utilização do compartilhamento de dados e informações entre instituições públicas de diferentes poderes e entes da federação.

Nesse ponto, a LGPD trouxe as seguintes previsões em seu artigo 26, caput Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: (...)

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

Portanto, ao considerarmos o rol de funções exercidas pelos Tribunais de Contas, é necessário observar fluxos específicos de tratamento de dados conforme as hipóteses presentes nos artigos 25 e 26 acima mencionados, assim como a dissociação em classes de dados.

Assim, a adaptação das operações dos Tribunais de Contas deve ser realizada para certificar a aderência com a LGPD, havendo necessidade de adoção de medidas de resguardo.

> *Nesse aspecto, é relevante revisar as atribuições infralegais previstas em normativas internas (tais como Resoluções, Instruções e Portarias), bem como as disposições inseridas em termos de cooperação, convênios, acordos de cooperação técnica, de modo a deixar mais clara a necessidade de utilização de dados e informações para suporte às ações de controle, adequando inclusive os procedimentos padrão de instrução e de fiscalização.*
> *Igualmente, mostra-se prudente a criação de controles, caso ainda não existam, para deixar claros os papéis e as responsabilidades dos profissionais que lidam com dados e informações em diversas fases, com a intenção de cumprir fielmente o que preveem os artigos 25 e 26 (caput) da LGPD.*
> *Dada a importância do uso de dados e informações para a atividade de controle externo, aqui inseridas não somente as de cunho pessoal, é recomendável que as Cortes de Contas avaliem a conveniência e oportunidade de criação de uma estrutura organizacional específica para a gestão de informações. Nos moldes dos* chief data officers, *presentes em agências públicas norte-americanas, tais estruturas prestam-se a tornar modernas e estáveis as atividades necessárias para suportar o uso e produção de informações para o controle externo em todo o seu ciclo de vida.*
> *É de se avaliar a necessidade de estabelecimento de fluxo de trabalho para integração e compartilhamento de informações com a ANPD. Como já referido anteriormente, uma vez instituída a ANPD e regulamentado o seu funcionamento, será necessário verificar os procedimentos de comunicação e estabelecer um processo de trabalho interno que dê suporte às eventuais interações com a agência.*

4.2. Experiência do TCU.

Através da *webinar* realizada na Escola de Contas do TCMSP, por iniciativa do grupo, tivemos contato com a experiência do TCU.

Em resumo, tem-se o seguinte[7]:

[7] Referências da *webinar* e de *e-mail* encaminhado pelo técnico do TCU que participou da implantação da LGPD.

Em 2019 o TCU instituiu grupo de trabalho, coordenado pelo Sr. Carlos Sampaio, para estudar o tema e propor ações necessárias[8].

A primeira iniciativa do grupo de trabalho foi fazer um diagnóstico detalhado das informações produzidas e custodiadas que contêm dados pessoais.

[8] ORDEM DE SERVIÇO-CCG Nº 03, DE 27 DE SETEMBRO DE 2019
Institui grupo de trabalho com o objetivo de estudar e propor regras para o tratamento de informações pessoais nos documentos públicos do Tribunal de Contas da União em conformidade com a Lei nº 13.709, de agosto de 2018.
Art. 2º *A análise inicial do grupo será dividida em coordenações setoriais, a depender da dimensão de impacto da LGPD no TCU.*
§ 1º *As coordenações setoriais serão atribuídas à unidade da Secretaria do TCU com maior afinidade com o conjunto de temas da coordenação.*
§ 2º *Cada coordenador setorial deverá preparar relatório dos achados e apresentar resumo aos demais membros, com propostas de solução para eventuais problemas encontrados, que serão usados para discussão e subsídio à elaboração do plano de ação do grupo de trabalho.*
Art. 3º *Os impactos da LGPD serão analisados nas seguintes dimensões*:
I - *impactos de controle externo, que abrangem o inventário de dados pessoais no exercício do controle externo e os procedimentos de coleta desses dados, bem como o processo de análise e cruzamento das bases de dados custodiadas pelo TCU*;
II - *impactos nos procedimentos administrativos, que abrangem o inventário de dados pessoais de autoridades, servidores e colaboradores no âmbito administrativo, os procedimentos de coleta desses dados e a análise dos dados disponibilizados na transparência administrativa*;
III - *impactos tecnológicos, que abrangem o apoio às unidades de negócio no inventário de dados pessoais, o apontamento de eventuais alterações em sistemas do TCU, a aquisição de soluções para melhoria da segurança dos dados e revisão de controles de acesso tecnológicos vigentes*;
IV - *impactos jurídicos, que abrangem a análise das interseções normativas legais e infralegais da LGPD, as eventuais mudanças em normativos internos, bem como a análise dos papéis previstos nessa nova lei*; e
V - *impactos nas informações de capacitação e treinamento, que abrangem o inventário de dados pessoais armazenados de terceiros nos processos de trabalho de capacitação e treinamento.*
Parágrafo único. *O inventário de dados pessoais deverá conter pelo menos*:
a) *identificação da informação pessoal armazenada*;
b) *local de armazenamento da informação*;
c) *rol de sistemas que fazem uso da informação pessoal*; e
d) *grupo de pessoas que tem acesso à informação.*
(...)
§ 1º *A redação do plano de ação proposto pelo grupo será elaborada pelo representante da Seplan, com subsídios nas informações enviadas pelos coordenadores setoriais.*
§ 2º *Ficam os coordenadores setoriais autorizados a incluir possíveis impactos nas respectivas dimensões, convidar outros servidores a participar das reuniões e a prestar apoio às atividades, se necessário.*
§ 3º *As atividades do grupo de trabalho serão realizadas sem prejuízo das demais atribuições dos participantes.*
Art. 5º O relatório final do grupo de trabalho e os produtos dele decorrentes serão submetidos à apreciação da CCG.

A Consultoria Jurídica do Tribunal (Conjur) auxiliou emitindo notas técnicas que respondiam a dúvidas da equipe e iluminavam o caminho a ser percorrido.

Resumidamente, a Conjur aduz que a base legal para tratamento das informações é o art. 23 da própria Lei Geral de Proteção de Dados Pessoais, que se refere ao cumprimento das atribuições legais conferidas à instituição.

Assim, o tratamento de dados pessoais se daria por força do cumprimento da missão institucional, afastando a necessidade de consentimento, prevista no inciso I do art. 7, da LGPD.

O inventário de informações foi também etapa fundamental para estabelecimento de ações emergenciais e de médio e longo prazo, sendo que o volume de informações armazenadas em diferentes formatos, repositórios e com regras de acesso distintas é significativo.

Em 2018 o TCU já tinha iniciado o desenvolvimento de um novo sistema informatizado de gestão de ações educacionais e esse sistema já nasceu com preocupações de segurança da informação e funcionalidades que permitem que o usuário possa consultar e alterar suas informações pessoais. A primeira versão desse sistema foi implantada em outubro de 2019 e o sistema tem sido evoluído para abranger todas as informações produzidas e custodiadas no Tribunal.

4.3. Experiência de outros Tribunais de Contas.

Com o auxílio da Subsecretaria de Fiscalização e Controle, diversos Tribunais de Contas foram consultados, via grupo no WhatsApp, sobre as providências adotadas para a implantação da LGPD.

Segue abaixo a relação dos Tribunais que apresentaram resposta e os respectivos conteúdos, nos termos enviados:

Com relação à implementação da LGPD:	**TCE-MG**	**TCE-RN**	**TCM-GO**	**TCE-AM**
1- O mapeamento de dados está sendo feito? Se sim, com pessoal terceirizado ou com pessoal interno?	*Sim. Cabe destacar que é um levantamento preliminar, que está sendo feito com pessoal interno (servidores e terceirizados). O mapeamento de dados em sistemas ainda está sendo discutido.*	*Sim, com pessoal interno.*	*Sim, a TI do TCM-GO tem os dados mapeados, mapeamento realizado com pessoal interno.*	*Está realizando estudos técnicos preliminares para atender a LGPD.*
2- Está sendo desenvolvido algum sistema de TI para a adequação á LGPD? Se sim, está sendo desenvolvido internamente ou por terceirizado?	*Não. Primeiro tem que terminar o inventário de sistemas e dados. A ideia é ajustar os sistemas.*	*Não.*	*Sobre o sistema de TI, ainda não temos nada desenvolvido, até porque para atender a LGPD não basta só o sistema de TI. O TCM-GO criou uma comissão para analisar os impactos e o que é necessário para se adequar a LGPD. O estudo foi finalizado, está em processo de revisão pelo Superintendente de Informática.**	(Não houve resposta para a pergunta)
3- Existe alguma normatização ou manual de	*Não. Está em discussão.*	*Ainda não, mas a ideia deverá ser*	*O IRB elaborou um estudo que serve como um manual de*	(Não houve resposta para a pergunta)

implementação da LGPD? Se sim qual?		*discutida em próximas ações.*	*implementação, o qual utilizamos como base para o nosso estudo.*	

*Acrescentou, ainda, que: "*A Superintendência de Informática do TCM-GO está preparando as adequações dos sistemas a LGPD, ainda existem várias questões jurídicas que deverão ser sanadas para um melhor posicionamento".*

4.4 Relatório do Grupo de Estudo da Prefeitura Municipal de São Paulo[9].

Aos 03 de agosto de 2020 foi publicado no DOC a conclusão do Relatório final do Grupo de Trabalho da Prefeitura Municipal de São Paulo, que articulou as ações da implantação da LGPD.

Em contato com o Chefe de Gabinete da Controladoria do Município, nos foi disponibilizado o número do processo SEI[10], no qual o Grupo de Estudo reuniu suas ações e anexou o Relatório final e a proposta de Decreto Municipal, posteriormente publicado sob o nº 59.767/2020.

Síntese da minuta do relatório de atividades do grupo intersecretarial instituído pela Portaria SGM 237, de 6 de setembro de 2019:

- A Lei nº 13.709, de 14 de agosto de 2018 possui como finalidade o estabelecimento das normas sobre o tratamento de dados pessoais pelas pessoas naturais ou pessoas jurídicas de direito público ou privado, bem como os instrumentos de proteção dos direitos fundamentais relacionados à liberdade e privacidade dos cidadãos.

[9] Documento anexo.
[10] Processo SEI nº 6023.2019/0002998-9.

- É necessária a constituição de estruturas de governança pública de dados e privacidade e, também, a elaboração de uma política de proteção de dados e privacidade para o estabelecimento dos princípios, diretrizes, procedimentos internos, padrões de respostas a incidentes, gestão de riscos, mapeamento, classificação dos dados, procedimentos de exclusão de dados solicitada pelos cidadãos, e outras ações que possam ser identificadas como fundamentais para essa adequação, identificando as atribuições e responsabilidades quanto à realização do controle sobre as atividades realizadas pelos servidores públicos em suas áreas de atuação, incentivando o engajamento dos mesmos nas medidas de proteção de dados, principalmente com a realização de capacitações e treinamentos para disseminação de boas práticas.
- O Relatório de Atividades do Grupo de Trabalho Intersecretarial, instituído pela Portaria SGM 237, de 06 de setembro de 2019, teve como finalidade apresentar (i) a sugestão de minuta do Decreto Municipal elaborada como resultado dos trabalhos realizados e (ii) os temas relevantes identificados nos estudos da LGPD e no desenvolvimento do trabalho do GTI.

No âmbito da Administração Indireta, destaca-se que a PRODAM firmou contrato de prestação de serviços de consultoria especializada para implantação da LGPD, bem como para capacitação de servidores (documento anexo - doc. 02).

4.5. Site do Tribunal de Justiça do Estado de São Paulo.

Por meio do site http://www.tjsp.jus.br/LGPD o TJSP trouxe algumas informações sobre a implantação da LGDP, bem como informações aos usuários no tocante à proteção de dados.

Na data de 20 de agosto de 2020, a coordenadora do grupo realizou reunião (*conference call)* com o Desembargador Dr. Rubens Rihl do TJSP, que deu início ao grupo de estudos daquele Tribunal para as adequações à LGPD.

Foi informado que 86 servidores integram o grupo da LGPD e ao menos duas empresas terceirizadas estão auxiliando no processo de anonimização e adaptação dos sistemas de tecnologia da informação.

Para obter maiores detalhes sobre a atuação do grupo e dos terceirizados, o Desembargador sinalizou a possibilidade de ser firmado convênio entre TCMSP e TJSP, objetivando a troca de experiência. Para que isso seja possível, é necessário entrar em contato com Juiz Assessor da Presidência, Dr. Fernando Tasso, que hoje é o coordenador da implantação da legislação no TJSP.

As Portarias 9.912/20 e 9.913/20 foram publicadas aos 08.09.20. A primeira normatizou o órgão *Encarregado pelo Tratamento de Dados Pessoais do Poder Judiciário de São Paul*o e a segunda designou os magistrados e servidores para integrar o novo órgão (documentos anexos – 03 e 04).

5. Normativos do TCMSP que podem ser impactados pela implantação da LGPD.

Os seguintes normativos do TCM foram selecionados:

NORMA	EMENTA
Instrução 01/2020 (aprovada pela Resolução 01/2020) *	Estabelece diretrizes gerais sobre a Política de Segurança de Informação no âmbito do Tribunal de Contas do Município de São Paulo.
Instrução 03/2016 (aprovada pela Resolução 15/2016) *	Dispõe sobre o acesso às informações dos processos em tramitação e dá outras providências.
Ordem interna de Regulamentação de Serviços 01/2020	Dispõe sobre o controle formal de regularidade da instrução de processos físicos de apreciação de aposentadorias e pensões, previamente ao arquivamento dos autos.
Ordem Interna 17/2019*	Dispõe sobre o requerimento de informação, juntada, vista, cópia e certidão de objeto e pé de processos arquivados no Tribunal de Contas do Município de São Paulo.
Ordem interna 15/2019*	Institui o "Manual de Classificação de Atos para o Sistema de Processo Eletrônico", nos termos do § 6º do art. 7º da Resolução nº 16/2018.
Ordem interna 03/2019*	Dispõe sobre procedimentos para desentranhamento de documentos nos processos físicos e eletrônicos no TCMSP.
Ordem interna 16/2018*	Regulamenta as normas previstas no Capítulo IX do Regimento Interno, que cuida de concessão de vistas, fornecimento de cópias de processo e juntada de documentos.
Ordem interna 14/2018*	Disciplina a tramitação de formulários de requisições por meio digital.
Ordem interna 13/2018	Dispõe sobre a autuação dos processos de prontuários de servidores antigos e novos, considerando a implantação do Sistema de Processo Eletrônico (e-TCM).

Ordem interna 12/2018*	Dispõe sobre a tramitação de documentos e processos físicos e eletrônicos.
Ordem interna 11/2018*	Define procedimentos que serão adotados para a gestão e controle dos documentos e processos físicos após a implantação do Sistema de Processo Eletrônico (e-TCM).
Portaria SG/GAB Nº 04/2020 *	Estabelece procedimentos com vistas ao cumprimento da Resolução nº 29/2019 e da Lei de Acesso à Informação no que tange à classificação de informações e dá outras providências.
Portaria 04/2018	Estabelece regras para a Unidade Técnica de Protocolo e Autuação relativas à implantação do Sistema de Processo Eletrônico (e-TCM).
Resolução 27/2019	Acrescenta o § 6º ao artigo 7º da Resolução nº 16/2018, que dispõe sobre o Processo Eletrônico no âmbito do Tribunal de Contas do Município de São Paulo (e-TCM).
Resolução 29/2019*	Dispõe sobre o acesso e divulgação das informações produzidas ou custodiadas pelo Tribunal de Contas do Município de São Paulo, bem como sobre a classificação das informações quanto à confidencialidade.
Resolução 16/2018	Dispõe sobre o Processo Eletrônico no âmbito do Tribunal de Contas do Município de São Paulo (eTCM).
Resolução 20/2018*	Dispõe sobre o Portal do Jurisdicionado e dá outras providências.
Resolução 15/2016*	Aprova a Instrução nº 03/2016, que dispõe sobre o acesso às informações dos processos em tramitação e dá outras providências.
Resolução 05/2016	Dispõe sobre o acesso às informações dos processos em tramitação e dá outras providências.
Resolução 06/2014*	Institui a Ouvidoria Digital do Tribunal de Contas do Município de São Paulo.
Resolução 03/2002 (última atualização: Resolução 07/2020)	Regimento Interno do TCMSP

Da análise dos normativos relacionados, encontram-se marcados com * aqueles que possivelmente serão impactados com a LGPD, podendo haver a necessidade de adequá-los.

Destaca-se, ainda, a necessária edição de Portaria de nomeação do *encarregado*, função que será detalhada no tópico 10.

6. Mapeamento das áreas do TCM - *Data Flow Map*

Após estudos preliminares da LGPD, compreendeu-se que a identificação dos dados pessoais e de quais ações os circundam seria necessária para que pudéssemos dar continuidade aos trabalhos de adequação à lei.

Assim, foi convencionado que o passo inicial seria o reconhecimento e o mapeamento da circulação, do tratamento e do acesso a dados pessoais (*data flow map*), nas diferentes áreas do Tribunal, por meio de um formulário a ser preenchido por determinados(as) servidores(as).

O formulário é composto por:

(a) um glossário de termos explicativos; e
(b) questões para resposta.

O glossário, feito com base no já mencionado art. 5º da LGPD, contém termos essenciais à compreensão da norma, como dados pessoais e dados

pessoais sensíveis, armazenamento, tratamento, titular e operador. A ideia central do glossário é a familiarização dos servidores com a terminologia legal e a apropriação dessa terminologia para o adequado preenchimento do formulário.

O modelo adotado para o desenvolvimento do formulário foi o *Google Forms* e a Chefia da AJCE, bem como o Secretário Geral foram devidamente consultados antes do início do mapeamento.

Em reunião de distribuição de tarefas, cada integrante do grupo ficou responsável por entrar em contato com o coordenador/chefe de uma ou mais áreas a serem mapeadas.

Com os resultados obtidos e consignados neste relatório, pode-se dar como atendido o art. 4º, do Decreto Municipal nº 59.767/2020[11].

6.1 Informações obtidas pela aplicação de formulário

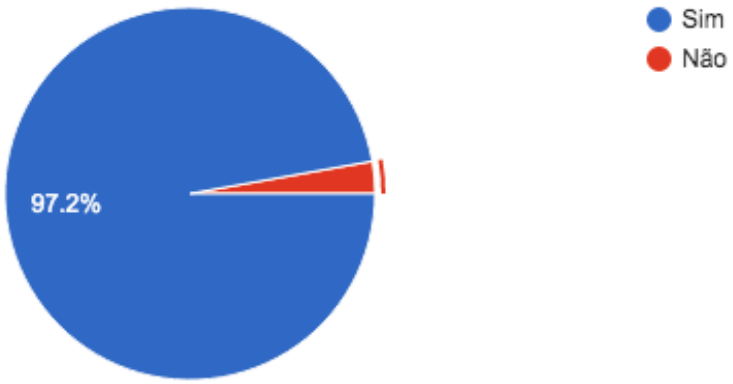
Foi apresentado um questionário[12] para áreas do Tribunal[13], com a ideia de se obter um mapeamento dos fluxos de dados pessoais que são coletados e que transitam pelo órgão, composto por dezoito perguntas.

[11] Art. 4º *O Poder Executivo Municipal, por meio de suas Secretarias e Subprefeituras, nos termos da Lei Federal nº 13.709, de 2018, deve realizar e manter continuamente atualizados*:
I – *o mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais em suas unidades*;
II – *a análise de risco*;
III – *o plano de adequação, observadas as exigências do art. 15 deste decreto*;
IV – *o relatório de impacto à proteção de dados pessoais, quando solicitado.*
(...)

[12] Questionário e respostas em anexo - docs 05.

Junto ao questionário, foi apresentado um glossário para que as áreas envolvidas tivessem acesso aos conceitos descritos na LGPD, de modo a auxiliá-las na etapa do mapeamento. O Grupo de Estudos também permaneceu à disposição para esclarecimentos.

Das áreas consultadas, 35 afirmaram ter acesso a dados pessoais (97,2%), enquanto uma (01) afirmou não ter acesso (2,8%).



Em relação à listagem de dados pessoais que as áreas têm contato, as respostas foram as seguintes:

[13] Áreas que responderam o questionário: Gabinete da Presidência, Gabinete do Conselheiro João Antonio, Gabinete do Conselheiro Roberto Braguim, Gabinete do Conselheiro Domingos Dissei, Gabinete do Conselheiro Maurício Faria, Gabinete do Conselheiro Edson Simões, Secretaria Geral, Assessoria Jurídica de Controle Externo, Comissão de Jurisprudência, Subsecretaria de Fiscalização e Controle, Coordenadoria I, Coordenadoria II, Coordenadoria III, Coordenadoria IV, Coordenadoria V, Coordenadoria VI, Coordenadoria VII, Coordenadoria VIII, Núcleo de Governança e Gestão (NGG) e seus escritórios (EMPP e ETQC), NTI - Unidade Técnica de Suporte ao Usuário, Unidade Técnica de Desenvolvimento de Sistemas, Subsecretaria Administrativa, Coordenadoria Administrativa, Coordenadoria de Contabilidade e Finanças, Coordenadoria Processual, Coordenadoria de Recursos Humanos, GRT/URH, Serviço de Saúde, Ouvidoria, Assessoria de Imprensa, Cerimonial, Controladoria Interna, Unidade técnica da EC – TI, Setor Administrativo da Escola de Gestão e Contas, Unidade Técnica de Biblioteca e Documentação – UTBD e Guarda Civil Metropolitana.

"- Quando é necessária informação sobre algum servidor para questão de férias ou licença médica, principalmente.

- Nome, sobrenome, data de nascimento, endereço residencial, *e-mail*, CPF e RG dos alunos e professores da EGC.

- Nomes completos e remuneração dos servidores.

- Geralmente, nome, sobrenome, endereço eletrônico (*e-mail*), CPF, RG, registro de entidades de classe a que pertence, tais como OAB ou CREA, registro funcional, etc.

- Dados constantes nos processos da Prefeitura: nome, sobrenome, idade, endereço residencial ou eletrônico (*e-mail*), CPF, RG, CNH, registro de entidades de classe, registro funcional, dados de localização, placas de automóvel. Dados provenientes dos sistemas como Átomo e upLexis.

- Nome, sobrenome, endereço eletrônico (*e-mail*), CPF, CNH, registro funcional, placas de automóvel, dentre outros.

- A EGC possui o cadastro de cada participante e nele contém nome, CPF, data de nascimento, *e-mail* para contato e telefone para contato.

- nome, sobrenome, RF, end eletrônico, hollerith e vida funcional.

- a) Documentos e informações pessoais inseridos em processos de fiscalização e em pedidos administrativos no TCMSP. b) Informações disponíveis em sistemas utilizados pelo TCMSP. c) Informações dos servidores do TCMSP disponíveis no CRH.

- *E-mail*, telefone, RG, CPF, RF (registro funcional).

- Nome, sobrenome, idade, endereço residencial e eletrônico(*e-mail*), CPF, RG, Registro Funcional, dados acadêmicos e biográficos.

- Nome, registro funcional e e-mail de servidores da SME, SMC e Seme, Fundatec e Theatro Municipal.

- nome, sobrenome, endereço, idade, telefone.

- Nome, sobrenome, CPF e identidade de servidores que participaram de cursos solicitados por nós (eventualmente).

- nome, sobrenome, apelido, idade, endereço residencial ou eletrônico (*e-mail*), CPF, RG, título de eleitor, CNH, registro de entidades de classe a que pertence, tais como OAB ou CREA, registro funcional, podendo incluir também, dados de localização, placas de automóvel, número de IP (*Internet Protocol*), dados acadêmicos, dentre outros.

- De maneira restrita, pois como temos acesso a relatórios de Auditoria, pela natureza do trabalho da AI de divulgação das atividades do Tribunal, temos, de certo modo, acesso ao nome dos agentes públicos municipais e/ou prestadores de serviços que são eventualmente citados nas auditorias.

- Informações inerentes a alguns dos sistemas internos do TCMSP, principalmente nos bancos de dados SQL-Server. Geralmente em ambiente de desenvolvimento ou homologação, mas em casos eventuais até mesmo em ambiente de produção.

- Todos os dados pessoais descritos no glossário.

- Dados dos servidores públicos do TCMSP e dos servidores dos Órgãos da Administração Direta e Indireta destinatárias do controle externo deste TCMSP.

- Nome, sobrenome, endereço eletrônico (*e-mail*), registro funcional, lotação, número de IP (Internet Protocol).

- Nome, CPF, número de outros documentos (RG, nº pensão, título de eleitor, RF, OAB, CREA, CRC, CRM, CRMV), endereço, telefones, *e-mail.*

- Todos informados no glossário e outros.

- Salários, endereços, etc...

- Mais especificamente do efetivo da GCM comissionado nesta Corte.

- Nomes das partes envolvidas nos processos sob análise do TCMSP.

- Dados constantes nos processos do TCM e da Prefeitura: nome, sobrenome, idade, endereço residencial ou eletrônico (*e-mail*), CPF, RG, CNH, registro de entidades de classe, registro funcional, dados de localização, placas de automóvel. Dados provenientes dos sistemas como Átomo.

- Nome, sobrenome, idade, endereço residencial ou eletrônico (*e-mail*), CPF, RG, título de eleitor, registro de entidades de classe a que pertence, tais como OAB ou CREA, registro funcional, podendo incluir também, dados acadêmicos.

- Nome, sobrenome, idade, endereço residencial ou eletrônico, CPF, RG, Registro Funcional, dados acadêmicos e do histórico profissional.

- * No sistema Átomo Radar, é possível visualizar nome completo, RG e CPF de sócios de empresas e dirigentes de Organizações da Sociedade Civil. * No sistema Upminer (externo e pago) é possível visualizar vários dados pessoais como nome completo, data de nascimento, RG, CPF,

endereço, telefone, *e-mail*, idade, sexo, nome da mãe, titularidade de empresas ou posição em organizações sociais, locais em que a pessoa trabalha/trabalhou, renda presumida, classe social, cheques sem fundo, restrições no SPC, protestos, propriedade de imóveis e propriedade de veículos.

- Documentos pessoais dos servidores públicos constantes nos processos de aposentadoria e pensões, assim como suas remunerações. Também acesso a documentos pessoais e informações de folha de pagamento dos servidores para as auditorias de pessoal.

- Nome, estado civil, RG e CPF, endereço, telefone, currículo - formação acadêmica e profissional e experiências profissionais.

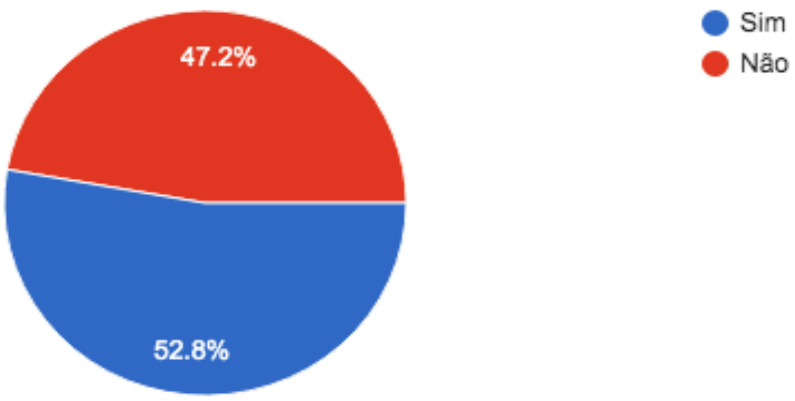
- Nome, qualificação, cargo.

- Dados pessoais genéricos constantes dos processos, principalmente aposentadorias.

- O gabinete da presidência não possui qualquer acesso direito a dados pessoais nem realiza tratamento deles. Ele apenas recebe de forma passiva, por impulso dos órgãos subordinados à presidência, processos administrativos, como pedidos de aposentadoria, pedidos de afastamentos, pedidos com base no art. 6°, XIV da Lei Federal n. 7.713/88, recursos em procedimentos licitatórios etc., todos já instruídos pelos órgãos técnicos, e que exigem a subscrição do presidente. Em alguns casos, o próprio interessado nesses processos fornece dados pessoais, como anexo de RG, CPF, geralmente porque necessita dessa documentação para instruir o pedido e comprovar o que é pleiteado. A análise dos dados fornecidos é feita de forma objetiva, independentemente do sujeito que a fornece, e apenas para verificar se estão presentes os requisitos fáticos e jurídicos para o que é pleiteado e para verificar se toda a instrução que ocorreu no Tribunal está correta. É mantido o devido sigilo em todos esses casos".

Sobre os dados pessoais sensíveis[14], 17 áreas afirmaram não ter contato (47,2%), enquanto 19 áreas responderam ter contato (52,8%).

[14] São aqueles relacionados às características da personalidade do indivíduo e às suas escolhas pessoais, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dados relativos à saúde ou à vida sexual, dado genético ou biométrico, dentre outros).



Em relação à listagem de dados pessoais sensíveis que as áreas têm contato, as respostas das respectivas áreas foram as seguintes:

> "- Setor Administrativo da Escola de Gestão e Contas: gênero;
>
> - Secretaria Geral: Dados pessoais, origem racial ou étnica (comissão do concurso), filiação a sindicato ou a organização política, dados relativos à saúde;
>
> - Coordenadoria I: Raça, gênero, filiação partidária;
>
> - Unidade Técnica de Biblioteca e Documentação: Gênero;
>
> - Serviço de Saúde: dados relativos à saúde, doenças e vida sexual;
>
> - Coordenadoria IV: Nome, e-mail, formação e registro de classe;
>
> - Ouvidoria: Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dados relativos à saúde ou à vida sexual;
>
> - Unidade Técnica de Desenvolvimento de Sistemas: Não temos necessariamente contato direto com esse tipo de informação, embora algumas das informações que constam nas bases de dados a que temos acesso possa ter caráter sensível;
>
> - Subsecretaria Administrativa: A maioria dos informados no glossário;
>
> - Coordenadoria Processual: Filiação a sindicato;
>
> - Coordenadoria de Recursos Humanos: origem racial ou étnica, filiação a sindicato, dados relativos à saúde, dado biométrico, entre outros que em

uma situação especial possa vir a ser necessário arquivamento em prontuário;

- Guarda Civil Metropolitana: origem racial ou étnica e convicção religiosa;

- Subsecretaria de Fiscalização e Controle: Filiação a sindicato, dados relativos à saúde;

- Assessoria Jurídica de Controle Externo: respondeu que tem acesso;

- GRT/URH: Informações da vida pessoal do indivíduo, no que se refere às questões levantadas nos laudos psicológicos do processo seletivo, nos relatórios de avaliação da GIEP, assim como informações relacionadas aos relacionamentos interpessoais do ambiente de trabalho;

- Gabinete do Conselheiro Mauricio Faria: São as informações encontradas em processos de aposentadoria e pensão que constituem dados relativos à saúde ou à vida sexual dos interessados

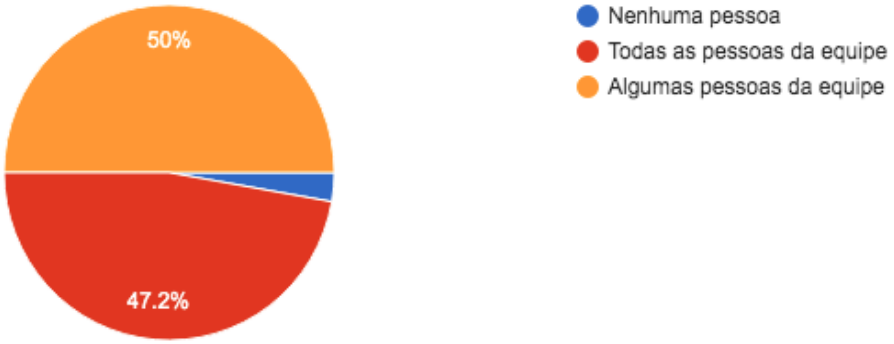
- Coordenadoria III: RG, CPF, endereço, dados cadastrais em geral, remuneração de servidores;

- Gabinete do Conselheiro Edson Simões: respondeu que tem acesso, mas não preencheu o item para especificar;

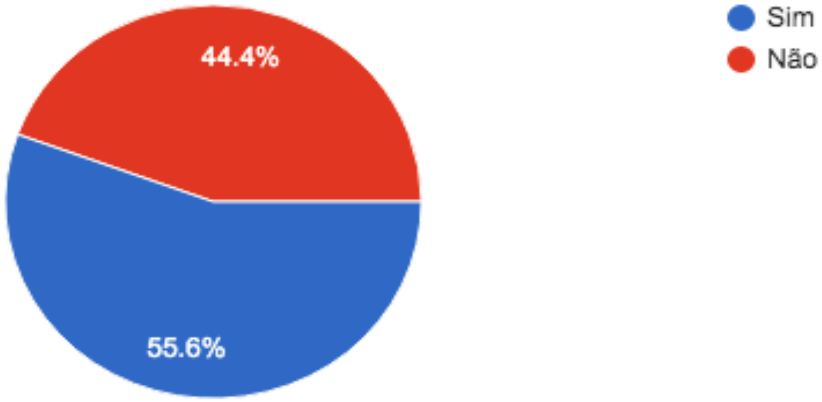
- Presidência: O gabinete da presidência não possui qualquer acesso direito a dados pessoais nem realiza tratamento deles. Ele apenas recebe de forma passiva, por impulso dos órgãos subordinados à presidência, processos administrativos, como pedidos de aposentadoria, pedidos de afastamentos, pedidos com base no art. 6°, XIV da Lei Federal n. 7.713/88, recursos em procedimentos licitatórios etc., todos já instruídos pelos órgãos técnicos, e que exigem a subscrição do presidente. Em alguns casos, o próprio interessado nesses processos fornece dados pessoais, como laudos médicos, geralmente porque necessita dessa documentação para instruir o pedido e comprovar o que é pleiteado. A análise dos dados fornecidos é feita de forma objetiva, independentemente do sujeito que a fornece, e apenas para verificar se estão presentes os requisitos fáticos e jurídicos para o que é pleiteado e para verificar se toda a instrução que ocorreu no Tribunal está correta. É mantido o devido sigilo em todos esses casos."

Quanto às pessoas que têm acesso a dados pessoais e a dados pessoais sensíveis: a) para 18 áreas (50%), a resposta foi "algumas pessoas da equipe"; b)

para uma (01) área (2,8%), a resposta foi “nenhuma pessoa”; e c) para 17 áreas (47,2%), a resposta foi “todas as pessoas da equipe”.



Quanto ao acesso a dados anonimizados[15]: a) 16 áreas (44,4%) responderam que não têm acesso; e b) 20 áreas (55,6%) responderam que têm acesso.



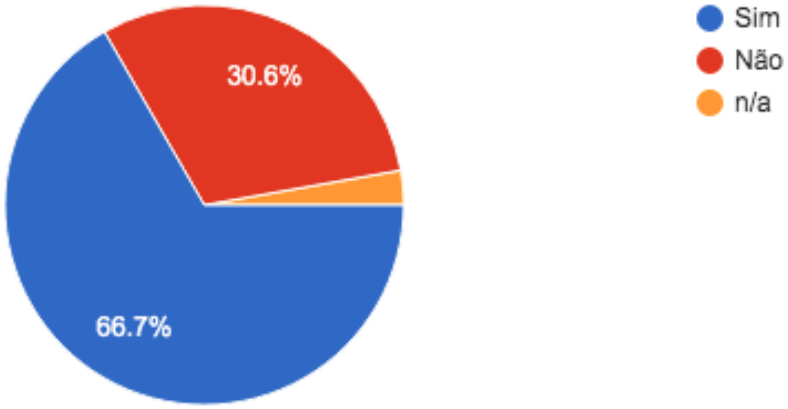
Sobre dar tratamento a algum tipo de dado pessoal:

a) 11 áreas (30,6%) responderam que não dão tratamento;

[15] É o dado relativo a titular que não possa ser identificado. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta.

b) 24 áreas (66,7%) responderam que dão tratamento;

c) Uma (01) área (2,8%) respondeu “n/a”;



Perguntadas diretamente sobre quais ações as áreas realizam, para caracterização de tratamento, apontaram a realização do que segue:

- Acesso;

- Processamento e transmissão;

- Eventualmente dados pessoais que constam nos processos da Prefeitura são anexados nos nossos processos;

- Coleta, reprodução e arquivamento/armazenamento basicamente;

- A EGC produz relatórios (Lista de presença, lista de portaria) em que contém a informação do nome da pessoa. Nesses relatórios não há informação de dados pessoais como CPF, telefone, e etc. Mas, em um dos relatórios denominado KIT, há a informação de *e-mail* e empresa. Esse tipo de relatório é compartilhado apenas com o instrutor do curso;

- Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, comunicação, transferência, extração;

- Recepção, acesso, reprodução e controle da informação, coleta, classificação, reprodução, transmissão, arquivamento;

- Coleta, recepção, classificação, utilização, acesso, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação;

- Coleta de nome, registro funcional e e-mail de servidores de algumas secretarias para utilização nos relatórios e processo eletrônico;

- Coleta, produção, arquivamento e armazenamento;

- Repassar os dados dos servidores para a empresa que realizou o curso emitir os certificados;

- Recepção, utilização, acesso, reprodução, transmissão, distribuição, arquivamento, armazenamento, edição, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- Acesso, recepção, reprodução, transmissão, distribuição, principalmente em dados que são disponibilizados no nosso Site de Transparência, como Relação de Servidores, Cargos e Salários. (Nota: Todas informações em tese públicas, que nos são passadas por *e-mail* pela CRH para posterior publicação). E, eventualmente, auxiliamos a CRH na operação de alguns sistemas que eventualmente possam ter informações sensíveis, como no caso do Auxílio Reembolso de Saúde, em que temos que auxiliar a CRH na conciliação de valores pagos, por exemplo;

- Todos os tratamentos descritos no glossário;

- Tratamento de IP quando necessidade de mudança de equipamento ou gerenciamento remoto, alteração de senhas quando necessário por solicitação do usuário;

- Coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, arquivamento, armazenamento, edição, eliminação, controle da informação, modificação, difusão, extração;

- Todas;

- Efetuamos a coleta dos dados dos julgados publicados no DOC, acórdão, relatório e voto do relator. Em posse destes dados, produzimos um arquivo no qual são consolidadas todas as informações e concedemos o acesso aos interessados por intermédio de sua divulgação na internet na pagina do Tribunal (aba jurisprudência), onde é possível efetuar pesquisas por termos em todos os arquivos constantes da base de dados disponibilizada. Estamos planejando mudanças, mas hoje é assim que acontece;

- Recepção, acesso, distribuição e arquivamento;

- Coleta, avaliação, classificação e transmissão;

- Coleta, recepção, utilização, acesso, transmissão, classificação, avaliação, controle e armazenamento;

- Coleta, recepção, utilização, acesso, armazenamento, avaliação, transferência, difusão e extração;

- Recepção, acesso, transmissão, arquivamento, armazenamento, edição, avaliação ou controle da informação, comunicação e transferência;

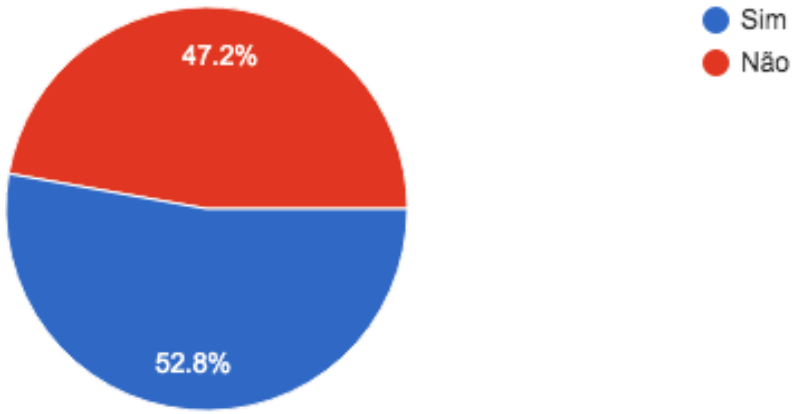
Posteriormente, no formulário (pergunta 14), foi realizada pergunta semelhante à supracitada, no entanto, desta vez, foram elencadas as ações listadas no conceito de tratamento de dados constante do art. 5º, inciso X da Lei nº 13.709/2018 (LGPD) e foram obtidas as seguintes afirmações:

Segundo as respostas fornecidas pelas áreas, as ações de coleta (50%), armazenamento (52,9%), recepção (55,9%), utilização (61,8%) e acesso (76,5%) são as atividades listadas pela LGPD mais realizadas atualmente no Tribunal de Contas do Município de São Paulo, enquanto componentes do conceito de tratamento de dados.

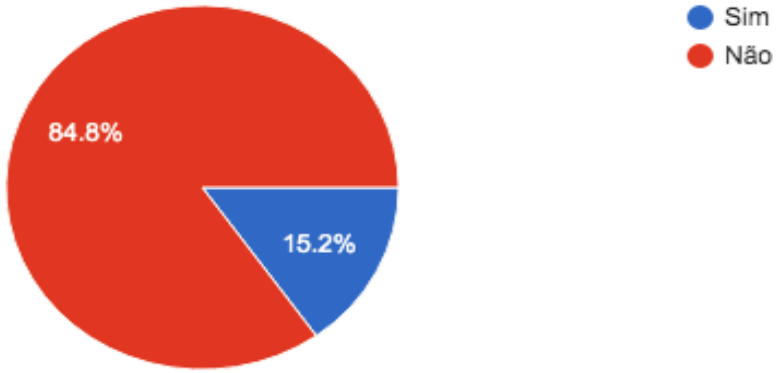
Entre 30% e 50% das respostas fornecidas, foram listadas as seguintes ações de tratamento: arquivamento (47,1%), transmissão (44,1%), reprodução (41,2%), processamento (35,3%), avaliação/controle de informação (35,3%) e comunicação (32,4%).

Já as ações listadas como menos realizadas – abaixo de 30% – foram: transferência/difusão/extração (26,5%), edição (23,5%), produção (23,5%), distribuição (23,5%), classificação (20,6%), eliminação (17,6%) e modificação (17,6%).

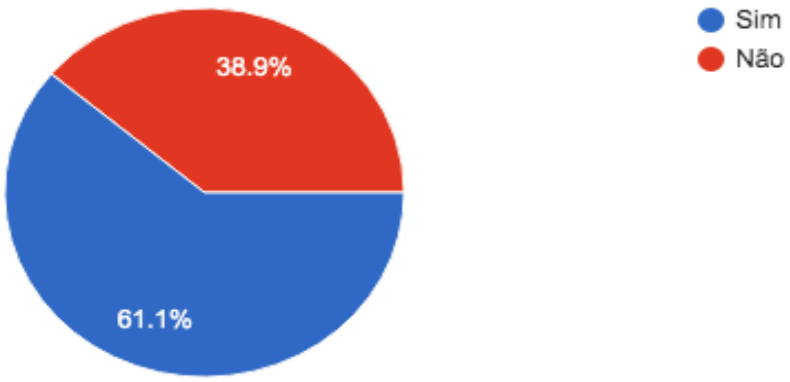
Sobre o armazenamento de dados pessoais, 17 áreas (47,2%) responderam que não armazenam, enquanto 19 áreas (52,8%) responderam que armazenam.



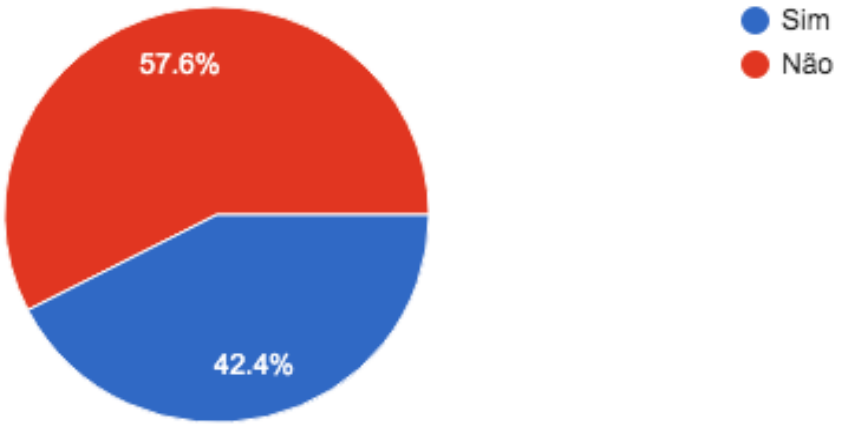
Quanto à existência de lapso temporal para a retenção de dados pessoais armazenados e eventual descarte, 28 áreas (84,8%) responderam que não há e cinco (05) áreas (15,2%) responderam que há. Indagadas sobre *qual* seria referido lapso temporal (prazo), apenas uma (01) área apontou prazo estimado (cem anos).



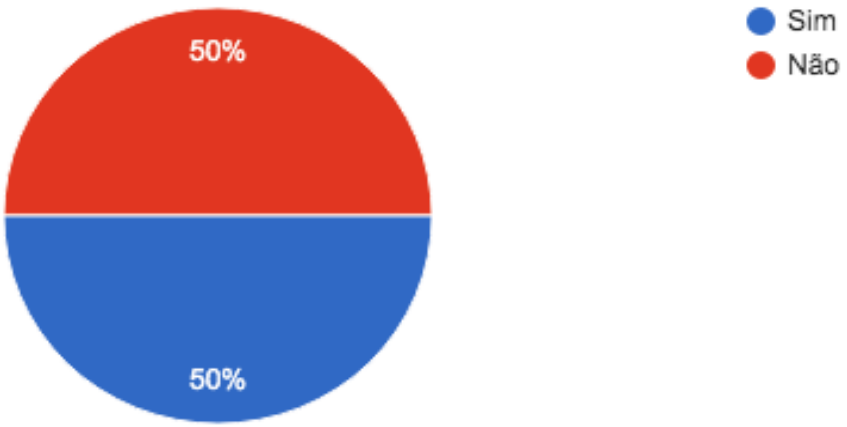
Em relação à utilização de dados de terceiros/externos: a) 14 áreas (38,9%) responderam que não utilizam; e b) 22 áreas (61,1%) responderam que utilizam.



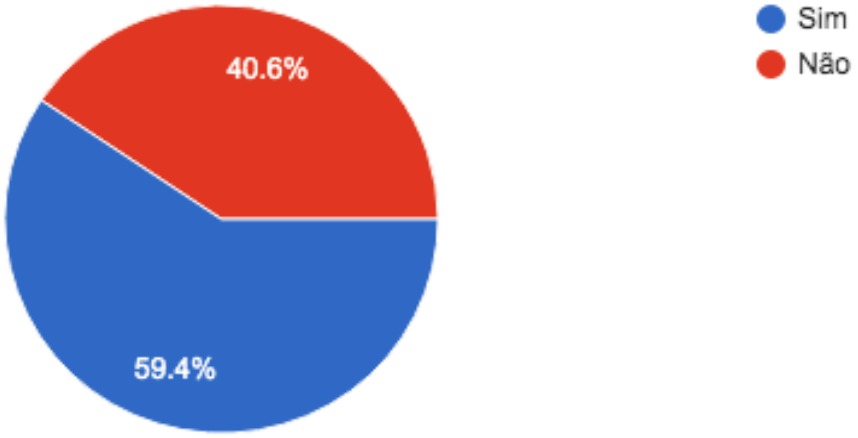
Quanto à integração do sistema utilizado com dados de sistemas externos, 14 áreas (42,4%) responderam que existe integração, enquanto 19 áreas (57,6%) responderam que não existe.



Sobre a disponibilização externa das informações armazenadas pelos sistemas, 16 áreas (50%) responderam que há disponibilização e 16 áreas (50%) responderam que não há.



Por último, no que se refere à utilização dos dados armazenados via sistema diretamente nas instruções processuais, 13 áreas (40,6%) responderam negativamente, enquanto 19 áreas (59,4%) responderam positivamente.



6.2 Reflexões sobre as informações obtidas

6.2.1 Conceitos

Em primeiro lugar, há uma reflexão conceitual. Parte dos conceitos apresentados pela LGPD afigura-se de difícil percepção por sua novidade no regime pátrio – exemplo claro, na própria lei, é a listagem de definições que consta do inciso X do art. 5º da Lei nº 13709/2018[16]. Se, de um lado, a lei enumera múltiplos processos e ações que compõem o tratamento de dados, por outro, termos que integram o referido rol, como processamento, arquivamento e controle de informação, por exemplo, são mencionados uma única vez no texto legal.

Em razão de tais inovações, buscamos inserir o glossário acima do questionário para orientar as respostas das pessoas designadas a respondê-lo dentro da parametrização exclusiva da norma, isto é, somente orientados pela literalidade da LGPD. Apesar disso, notamos algumas inconsistências nas respostas, o que nos parece de certa forma explicável diante das dificuldades que a implantação de uma nova cultura de proteção de dados ocasiona.

Exemplarmente, em resposta à pergunta sobre qual informação de dados sensíveis determinada área detinha, ou acessava, duas das quatorze respostas mencionaram documentos pessoais (RG e CPF), nome, endereço eletrônico,

[16] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

registro de classe e endereço físico – tais informações classificar-se-iam como dados pessoais não sensíveis. É relevante que se mencione a correção, uma vez que a lei diferencia o tratamento conferido a cada tipo de dado pessoal.

6.2.2. Acesso e Utilização

Ao confrontarmos os resultados apresentados nas questões 01 e 18, quais sejam, "acesso a dados pessoais" e "uso de dados pessoais em instrução processual" – processo aqui concebido na visão desenvolvida nas Leis Federal nº 9.784/1999 e Municipal 14.141/2006 –, tem-se que 35 áreas afirmaram ter acesso a dados pessoais, ao passo que, das 35, apenas 19 áreas utilizam-nos na instrução processual.

Onze[17] áreas que têm acesso a dados pessoais (resposta afirmativa à primeira pergunta) marcaram que não se utilizam de tais dados para instruir os processos administrativos com que trabalham – dentre estas, há ao menos cinco áreas[18] que marcaram que "coletam" dados em sua atividade.

Quatorze áreas afirmam ter acesso a dados pessoais sensíveis[19]. A natureza dos dados sensíveis elencados é muito variada: os substantivos listados no inciso II do art. 5º da LGPD[20] foram todos listados em algum grau de retenção e/ou acesso por distintas áreas do TCMSP. Os dados sensíveis mais

[17] Excluiu-se do montante o serviço de saúde dado que respeitam protocolo de sigilo próprio à área de saúde.
[18] GCM, EGC, UTBD, Jurisprudência e Controladoria Interna.
[19] CRH, GRT/URH, SG, Gabinete da Presidência do TCMSP, GCM, EGC, UTBD, AJCE, CP, GMF, GEES. UTDS-NTI, Serviço de Saúde e Ouvidoria.
[20] "*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*".

citados no levantamento foram: raça (cinco menções), filiação a sindicato (cinco menções), e dados relativos à saúde ou à vida sexual (quatro menções).

Quanto às pessoas que acessam, integrantes das unidades, há equilíbrio de respostas (questão cinco): dezessete áreas afirmam que todos têm acesso, enquanto dezoito afirmam que algumas pessoas têm acesso – deste grupo, oito áreas indicaram quais pessoas (*cargos/funções*) teriam acesso.

Ao se realizar cruzamentos das respostas à quinta questão, tem-se que treze áreas das dezoito que têm acesso limitado possuem acesso a dados pessoais sensíveis. Entre as treze áreas, encontram-se as oito áreas que indicaram os *cargos*/*funções* – o que demonstra adequação perante a LGPD, dada a requisição legal de clareza no fluxo de tratamento de dados e quem os pode acessar.

Enquanto isso, três áreas, nas quais todos têm acesso, detêm acesso a dados pessoais sensíveis – são elas: EGC (*gênero*), Coordenadoria Processual (*filiação a sindicato*) e Ouvidoria (*origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relativos à saúde ou à vida sexual*). Há que se analisar internamente a necessidade de haver acesso indiscriminado a dados pessoais considerados sensíveis dentro de cada área – com **particular ênfase** no caso apresentado para a Ouvidoria.

6.2.3 Tempo e Armazenamento

Uma questão emergente do levantamento é muito relevante para o desenvolvimento de políticas internas de segurança e de gestão de dados – trata-se do elemento *temporal* de retenção dos dados.

Em resposta à questão de número dez, **dezenove áreas afirmaram possuir** algum tipo de armazenamento de dados, no entanto, apenas **quatro** das dezenove afirmaram haver algum prazo para a sua eliminação e, destas, apenas **uma área** conferiu um prazo temporal (100 anos). Das mesmas dezenove áreas que armazenam dados, **quatro** estão entre as áreas que também afirmam não utilizar os dados em instrução processual[21].

Destaque-se que a resposta da Coordenadoria V ilustra perfeitamente a necessidade de sequência dos estudos[22] para a LGPD: a Subsecretaria de Fiscalização e Controle conjuntamente aos demais órgãos integrantes do exercício do controle externo do TCMSP deverão envidar esforços para definir prazo razoável e forma de armazenamento adequada aos documentos que contenham dados pessoais e dados pessoais sensíveis utilizados na elaboração dos atos de fiscalização e que fundamentam os papéis de trabalho da Auditoria.

Doze[23] das dezenove áreas que armazenam dados pessoais afirmam que a coleta é uma das ações que praticam no tratamento de dados (questão quatorze)

[21] GCM, EGC, UTBD e Controladoria Interna. Nesta pontuação, optou-se por excluir o Serviço de Saúde, dado que, inclusive em virtude de sigilo profissional, não instrui processos do TCMSP com dados pessoais e dados pessoais sensíveis dos servidores atendidos.
[22] Importante notar a resposta conferida pela Coordenadoria V: "O armazenamento via de regra se dá junto com os **papéis de trabalho**, seguindo, portanto, as diretrizes de prazo de armazenamento daqueles documentos."
[23] Coordenadoria I, SFC Coordenadoria III, CRH, GRT/URH, NGG, GCM, EGC, UTBD, CP, AJCE, GMF, Controladoria Interna – faz-se novamente a ressalva relativa ao serviço de saúde já anteriormente pontuada.

– destas doze, oito[24] afirmam não haver lapso temporal para a retenção do dado. Isto é, há oito áreas, dentre as doze, que afirmam armazenar dados pessoais, que afirmam coletá-los e que não dispõem de *lapso temporal* para a sua retenção.

6.2.4. Tratamento

Em resposta à pergunta de número oito, 24 das 35 áreas responderam que conferem algum tratamento a dados pessoais. Valendo-nos das análises numéricas já descritas, relativas à questão quatorze, tem-se que:

Em geral, as áreas do TCMSP acessam (76,5%) e utilizam (61,8%) dados pessoais, seja por coleta (50%), seja por recepção (55,9%) e armazenam os dados que coletam ou recebem (52,9%) e os arquivam (47,1%)[25]. As ações de reprodução (41,2%), processamento, controle e avaliação (35,3% cada uma) de dados pessoais permeiam significativamente também o fluxo do tratamento de dados no TCMSP – no entanto, as ações menos realizadas pelo fluxo de tratamento foram classificação (20,6%), eliminação (17,6%) e modificação (17,6%).

Um diagnóstico primário e superficial indicaria que o fluxo de dados pessoais no TCMSP se pauta em largas portas de entrada e de coleta de dados pessoais, que são utilizados, reproduzidos e processados no curso do tratamento,

[24] Coordenadoria I, Coordenadoria III, GRT/URH, NGG, EGC, UTBD, CP e GMF.
[25] Qual seria a diferença essencial entre **armazenar** e **arquivar**? Segundo o **Glossário da LGPD**, elaborado pelo **SERPRO** (https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd - acesso em set/2020):
*"**armazenamento** - ação ou resultado de **manter** ou **conservar em repositório** um dado*
arquivamento** - ato ou efeito de **manter registrado um dado** embora **já tenha perdido a validade ou esgotada a sua vigência" (grifos nossos)

mas cujo ciclo de vida (elemento *temporal* volta à tona) não é finalizado – assim, formam-se acúmulos de dados pessoais de distintas ordens que são utilizados internamente, sem, contudo, haver uma destinação final (eliminação, retirada de circulação e/ou *backup* externo).

6.3 Conclusões

Diante do resultado do mapeamento, bem como das atribuições de cada uma das áreas, parece-nos que demandam maior atenção: Secretaria Geral, Subsecretaria de Fiscalização e Controle, Assessoria Jurídica de Controle Externo, Serviço de Saúde, Coordenadoria de Recursos Humanos, GRT/URH, Presidência, Coordenadoria Processual, Escola de Gestão e Contas e Ouvidoria.

A partir das informações obtidas no formulário, há que se evidenciar as ações administrativas, e por extensão, as áreas que as performam, que demandam atenção imediata do Tribunal de Contas do Município de São Paulo para que se evitem potenciais violações à literalidade da norma (LGPD) – dado que as interpretações sedimentadas da lei ainda são incipientes. Expõem-se as conclusões a partir da **natureza do dado**:

DADO PESSOAL SENSÍVEL

Disposição Genérica: inicia-se pontuando que quaisquer áreas que **tenham contato com dados pessoais sensíveis** trabalhem para:

(a) estabelecer a **finalidade** do dado;

(b) se coletam, providenciar **consentimento** para acesso ao dado pessoal sensível ou a notificação de **consentimento** do dado armazenado;

(c) se armazenam ou exercem gestão, **delimitar** a quem o acesso é garantido;

(d) definir ciclo de vida do dado pessoal sensível apreendido: as digitais que marcam o ponto eletrônico, por exemplo, se houver aposentadoria do servidor que marca o ponto, referidos dados sensíveis deverão ter protocolo de eliminação; e

(e) se os **dados pessoais sensíveis** são acessados a partir de banco de dados de terceiro, garantir-se que a sua **coleta** e demais ações de tratamento tenham sido consentidas pelo detentor (*pessoa natural*).

Disposições Específicas: quanto à **Ouvidoria**, é premente que se reavalie a política de acesso, coleta, manutenção e reprodução de dados pessoais sensíveis.

Quanto à **Coordenadoria Processual** e à **Escola de Contas**, é premente que se estabeleça internamente quem poderá acessar os dados pessoais de estudantes, bem como reavaliar a necessidade de **coleta** de determinados dados.

DADOS PESSOAIS

Disposições Genéricas: o Tribunal de Contas do Município de São Paulo, nos atributos a ele instituídos por sua lei inaugural e pela lei orgânica do Município, bem como pela aplicação do paralelismo das formas e as disposições constitucionais, detém prerrogativas de utilização de dados pessoais no efetivo exercício da fiscalização do controle externo.

Nos termos dos artigos 7º, incisos II, III e VI, e §§3º e 4º, 23, *caput* e inciso I, 25, 26, *caput*, da própria LGPD:

> Art. 7º *O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses*:

(…)
II - *para o cumprimento de obrigação legal ou regulatória pelo controlador*;
III - *pela administração pública, 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, observadas as disposições do Capítulo IV desta Lei*;
(...)
VI - *para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)* ;
(…)

§ 3º *O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.*

§ 4º *É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.*

Art. 23. *O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado 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:*
I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

Art. 25. *Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.*

> Art. 26. *O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.*

A despeito da autorização legal, o Tribunal se circunstancia às regras gerais de tratamento de dados pessoais[26] e se obriga à atenção aos princípios constantes do art. 6º, da LGPD[27].

Assim, considerando-se que o mapeamento preliminar identificou numerosos focos de coleta de dados pessoais, há que se delinear:

---

26 **Art. 7º, §6º, LGPD:** "*A **eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei**, especialmente da observância dos princípios gerais e da garantia dos direitos do titular."*

27 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

(a) a atenção aos princípios, com destaque para a finalidade e a necessidade de se realizar tal coleta;

(b) revisão de métodos de coleta: *como se coletam os dados*; e

(c) se a finalidade for de exercício efetivo de obrigação legal, dispensa-se o consentimento, se for de outra natureza, há que se pensar em obtenção de **consentimento – livre e expresso**.

Considerando-se as ações de acesso, de reprodução, de extração, de utilização e de recepção:

(a) voltar-se para o modo de obtenção primário do dado;

(b) se a informação for entregue pelo próprio jurisdicionado, há que se ter em mente a potencialidade de se ocultar dados pessoais alheios ao devido andamento processual e/ou obter consentimento individual para o prosseguimento dos dados sem ocultação internamente (processo administrativo é, via de regra, público); e

(c) se o dado pessoal for obtido a partir de consulta a bancos de dados, analisar-se a natureza dos bancos utilizados (domínio público, natureza privada) e a eventual existência de consentimento das pessoas naturais afetadas.

Considerando-se as ações de arquivamento, armazenamento e eliminação:

(a) há que se **estabelecer ciclos** de vida dos dados pessoais internamente no Tribunal, levando-se em conta a finalidade e a necessidade de existência de determinados dados pessoais em bancos de dados;

(b) estabelecer política interna de proteção dos dados pessoais – com destaque para as áreas que concedem acesso indiscriminado a todos os seus integrantes;

(c) estabelecer política interna de acesso que garanta a finalidade para a qual o dado pessoal esteja sendo utilizado; e

(d) estudar prazos que sejam para arquivamento, para armazenamento e para eliminação de dados pessoais que amparem as atividades de fiscalização.

Por fim, as conclusões do mapeamento se amparam tão-somente no que fora apresentado pelas áreas, com os conceitos como os temos estabelecidos hodiernamente e as limitações que, consequentemente, guardam. As linhas gerais acima tracejadas cuidam das medidas necessárias para que o TCMSP se adeque sistemicamente à implementação da LGPD, é dizer, para que o Tribunal dialogue plenamente tanto com as regras da lei, quanto com as suas normas.

7. *Data protection by design*[28] (Privacidade por definição)

A LGPD, no seu artigo 46, determina que devem ser adotadas medidas técnicas, de segurança e administrativas que venham a garantir a segurança dos dados dos usuários contra acessos não autorizados, que se inserem nas providências a serem adotadas pelo TCMSP (item 10 e 11).

A privacidade dos dados pessoais passa a ser pensada como parte indissociável de qualquer atuação do TCMSP (incorporação na metodologia do trabalho), por meio da implementação de medidas apropriadas para proteção dos dados e da configuração de um sistema de segurança eficaz.

Passa-se a considerar a proteção de dados como indissociável do manuseio de informações pessoais constantes das bases de dados do Tribunal ou coletadas por qualquer dos servidores para fins de instrução processual ou para outra finalidade inerente à atuação do TCMSP.

Envolve, ainda, a escolha e treinamento da estrutura funcional (item 8), bem como a utilização de mecanismos tecnológicos para possível anonimização de dados (item 9), de modo que a tecnologia será elemento indispensável para implantação e adaptação à Lei.

[28] Trata-se de metodologia criada na década de 90 pela Comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian. Naquela época a especialista já imaginava que o avanço da tecnologia e a facilidade de comunicação possibilitariam uma coleta indiscriminada de informações pessoais e que, portanto, algum conceito deveria ser aplicado para que as corporações entendessem e aplicassem regras de privacidade em suas soluções e produtos oferecidos. A partir de 2010 diversas entidades ao redor do mundo começaram a divulgar e aplicar estes conceitos, como por exemplo a Autoridade Europeia de Proteção de Dados e a Federal Trade Comission nos Estados Unidos. Atualmente o privacy by design está incorporado na legislação europeia de proteção de dados (GDPR) e em nossa Lei Geral de Proteção de Dados (LGPD).

8. Escolha da estrutura funcional

Nos artigos 37 a 41 da LGPD, são detalhadas as competências e as responsabilidades do controlador, do encarregado e do operador.

O TCM deverá definir o seu papel como **controlador**, pessoa jurídica de direito público, respondendo diretamente pelo tratamento dos dados pessoais sob sua guarda no cumprimento de obrigação legal ou regulatória. As providências a serem adotadas foram enumeradas nos dois últimos tópicos deste relatório.

Nesse contexto, a competência para as atribuições da figura do controlador (entre elas a indicação da equipe técnica que deverá tomar decisões referentes ao tratamento de dados pessoais) deverá ser regulamentada pelo TCM[29].

Algumas responsabilidades do controlador já estão previstas na LGPD, como a de comunicar à ANPD (Autoridade Nacional de Proteção de Dados[30]) e aos titulares de dados pessoais a ocorrência de incidente de segurança que "possa acarretar risco ou dano relevante aos titulares".

Cumpre transcrever o conceito e as respectivas funções do controlador, operador e encarregado, trazidas pela LGPD, bem como pelo Decreto Municipal nº 59.767/2020:

[29] Com base na nota técnica nº 01/19 do Instituto Rui Barbosa.
[30] Estrutura criada pelo Decreto Federal nº 10.474/2020.

Lei nº 13.709/2018 - LGPD

Art. 5º *Para os fins desta Lei, considera-se*:

(...)

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

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

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

(...)

Art. 37. *O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse*.

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 adotados*.

Art. 39. *O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria*.

Art. 40. *A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência*.

Art. 41. *O controlador deverá indicar encarregado pelo tratamento de dados pessoais*.

§ 1º *A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador*.

§ 2º *As atividades do encarregado consistem em*:

I - *aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências*;

II - *receber comunicações da autoridade nacional e adotar providências*;

III - *orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais*; e

IV - *executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares*.

§ 3º *A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados*.

Decreto Municipal nº 59.767/2020.

Art. 2º *Para os fins deste decreto, considera-se*:

(...)

VI - *controlador: pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*;

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

VIII - *encarregado: pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)*;

(...)

Art. 5º *Fica designado o Controlador Geral do Município como o encarregado da proteção de dados pessoais, para os fins do art. 41 da Lei Federal nº 13.709, de 2018*.

Parágrafo único. *A identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, no Portal da Transparência, em seção específica sobre tratamento de dados pessoais*.

Art. 6º *São atribuições do encarregado da proteção de dados pessoais*:

I – *aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências*;

II – *receber comunicações da autoridade nacional e adotar providências*;

III – *orientar os funcionários e os contratados da Administração Pública Direta a respeito das práticas a serem tomadas em relação à proteção de dados pessoais*;

IV – *editar diretrizes para a elaboração dos planos de adequação, conforme art. 4º, inciso III deste decreto*;

V – *determinar a órgãos da Prefeitura a realização de estudos técnicos para elaboração das diretrizes previstas no inciso IV deste artigo*;

VI - *submeter à Comissão Municipal de Acesso à Informação (CMAI), sempre que julgar necessário, matérias atinentes a este decreto*;

VII – *decidir sobre as sugestões formuladas pela autoridade nacional a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais, nos termos do art. 32 da Lei Federal nº 13.709, de 2018*;

VIII – *providenciar a publicação dos relatórios de impacto à proteção de dados pessoais previstos pelo art. 32 da Lei Federal nº 13.709, de 2018*;

IX - *recomendar a elaboração de planos de adequação relativos à proteção de dados pessoais ao encarregado das entidades integrantes da Administração indireta, informando eventual ausência à Secretaria responsável pelo controle da entidade, para as providências pertinentes*;

X - *providenciar, em caso de recebimento de informe da autoridade nacional com medidas cabíveis para fazer cessar uma afirmada violação à Lei Federal nº 13.709, de 2018, nos termos do art. 31 daquela lei, o encaminhamento ao órgão municipal responsável pelo*

> *tratamento de dados pessoais, fixando prazo para atendimento à solicitação ou apresentação das justificativas pertinentes*;
>
> XI - *avaliar as justificativas apresentadas nos termos do inciso X deste artigo, para o fim de*:
>
> a) *caso avalie ter havido a violação, determinar a adoção das medidas solicitadas pela autoridade nacional*;
>
> b) *caso avalie não ter havido a violação, apresentar as justificativas pertinentes à autoridade nacional, segundo o procedimento cabível*;
>
> XII - *requisitar das Secretarias e Subprefeituras responsáveis as informações pertinentes, para sua compilação em um único relatório, caso solicitada pela autoridade nacional a publicação de relatórios de impacto à proteção de dados pessoais, nos termos do artigo 32 da Lei Federal nº 13.709, de 2018*;
>
> XII – *executar as demais atribuições estabelecidas em normas complementares*.
>
> § 1º *O Controlador Geral do Município terá os recursos operacionais e financeiros necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como acesso motivado a todas as operações de tratamento*.
>
> § 2º *Na qualidade de encarregado da proteção de dados, o Controlador Geral do Município está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com a Lei Federal nº 13.709, de 2018, com a Lei Federal nº 12.527, de 18 de novembro de 2011, e com o Decreto nº 53.623, de 12 de dezembro de 2012*.

Conforme já sinalizado anteriormente, no âmbito da Prefeitura do Município de São Paulo ficou designado o Controlador Geral do Município como o encarregado da proteção de dados pessoais.

Seguem outros exemplos da escolha da estrutura funcional feitas por órgãos públicos:

- PGE-RJ: Procurador Geral é o Encarregado da PGE[31].
- Ministério de Infraestrutura do Governo Federal: Ouvidor é o Encarregado do Ministério[32].
- TJ-PB: Gabinete da Presidência ficou designado para cuidar da LGPD - Encarregado servidor do Gab. da Presidência[33].
- TJ-SC: Desembargadora é a Encarregada[34].
- TJ-SP: Comissão Multissetorial[35].

9. Constatações inerentes à Tecnologia da Informação

Em atuação conjunta do grupo com o Núcleo de Tecnologia da Informação, foi efetivado um prévio levantamento das providências a serem tomadas em relação às adequações do e-TCM a fim de atender aos requisitos da LGPD.

Destaca-se que o Núcleo de Tecnologia da Informação e a Secretaria Geral são patrocinadores do projeto que tem como fim tratar das alterações necessárias no Sistema e-TCM para aderência às normas dispostas na LGPD (documento anexo- doc. 06).

[31] http://www.ioerj.com.br/portal/modules/conteudoonline/mostra_edicao.php?session=VWtWWk1FMXJUa0pSVlZsMFVWUk5lVTE1TURCTlZWWkdURlZKZDFGcldYUlNWVTEzVFd0Vk1WSnJSVFJOTUZwRw==&p=MjQ=&tb=dHJhdGFtZW50byBkZSBkYWRvcyBwZXNzb2FpcyYjMDEzOw==

[32] https://www.gov.br/infraestrutura/pt-br/assuntos/noticias/ultimas-noticias/ouvidor-e-designado-para-dar-tratamento-aos-dados-pessoais-dos-cidadaos-colhidos-pelo-ministerio

[33] https://www.tjpb.jus.br/noticia/seguranca-tjpb-em-fase-final-do-projeto-para-implantar-lei-geral-de-protecao-de-dados
https://www.tjpb.jus.br/protecao-de-dados-pessoais/encarregado

[34] https://www.tjsc.jus.br/web/ouvidoria/lei-geral-de-protecao-de-dados-pessoais/encarregado-pelo-tratamento-de-dados-pessoais

[35] http://www.tjsp.jus.br/Areas/LGPD/Content/Docs/Portaria_9885-19.pdf

Seguem os detalhes, trazidos pelo NTI, envolvendo os principais recursos do sistema que devem ser analisados como possíveis geradores de demandas de ajustes e melhorias:

Com o objetivo de analisar a necessidade de adequação do sistema de gestão de processos e documentos eletrônicos **(e-TCM)**, conforme a **Lei Geral de Proteção de Dados**, foi realizado levantamento dos principais recursos da ferramenta utilizados para registro, tratamento e consulta de dados relacionados ao cadastro de "pessoas" físicas e jurídicas, vinculados aos protocolos de processos e expedientes do TCM SP.

O levantamento teve como foco a necessidade de avaliar os recursos do sistema que tratam dados de "pessoa" e orientar os usuários do e-TCM sobre a sua responsabilidade quanto ao acesso e tratamento de dados classificados como "sensíveis" , segundo a LGPD, propondo ajustes que possam ser providenciados de acordo com a sua complexidade e urgência.

- **Identificação de dados sensíveis,** como por exemplo, dados pessoais que estão sujeitos a condições de tratamento específicas e que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados relativos à vida sexual ou orientação sexual da pessoa.
- **Anonimização de dados,** conforme o artigo 5º, inciso XI, da lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) que

define como anonimização a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado pessoal perde a possibilidade de associação, direta ou indireta, com o seu titular.

- **Orientações sobre a responsabilidade do usuário do sistema,** para compreensão do que são dados sensíveis. Para saber lidar com dados sensíveis é preciso compreender o que eles significam e a sua importância, sabendo que, basicamente, são informações pessoais, que podem comprometer pessoas a situações indesejáveis caso venham a ser divulgadas.
- **Outras possíveis providências de adequações para:**
  - Identificar onde é necessária aplicação de recursos como criptografia de dados e informações de forma que não sejam reconhecíveis à primeira vista.
  - Adequação de uso de senhas para proteger qualquer sistema, recurso de sistema (consultas externas, *links*, etc.) de acesso indevido.
  - Adoção de termos de confidencialidade, uma vez que apesar de serem confidenciais, muitos dados sensíveis precisam ser acessados todos os dias para executar algumas tarefas, como preencher solicitações de pedidos e conferir o status de algum serviço.
  - Adequação/ampliação de Redes Privadas Virtuais (VPN) e demais soluções adotadas a fim de ampliar os recursos de gestão de armazenagem e de acesso a dados classificados ou não como sigilosos.

- Manutenção da Politica de Segurança, com rígido controle de acessos, para alcançar o nível de segurança desejado para os seus dados sensíveis, considerando que, diferente do entendimento da grande maioria dos usuários, isso não diz respeito apenas a quem pode ou não entrar numa rede privada, mas também todo o controle de acesso como o histórico de *logins* e de ações realizadas dentro da rede, acompanhando o que cada usuário fez enquanto acessa os dados, levando a esclarecer erros humanos, além de identificar mais facilmente acessos ilegais.

- **Capacitação dos usuários** para evitar riscos, considerando que boa parte da segurança de informação depende diretamente dos usuários de sistemas que acessam bancos de dados todos os dias, podendo levar informações sigilosas para o seu computador pessoal, ou fornecer informações a outra pessoa, com ou sem conhecimento da ilegalidade. Senso assim, como primeira providência, a melhor solução, nesse caso, é capacitar e orientar os usuários do e-TCM e demais sistemas do TCMSP para que esse tipo de erro não seja cometido.
  - Uma alternativa para divulgação dessas diretrizes é o uso da própria solução e-TCM com a inclusão de orientação sobre a LGPD em cada tela de recurso que trata dados sensíveis.
  - Customização de página específica no portal do TCMSP para uso exclusivo de assuntos tratados pelo Projeto de Implantação da LGPD.

Recursos e-TCM:

1. Tela de *login* de usuários e-TCM.

   a. A tela de *login* do e-TCM apresenta, além da opção de acesso ao sistema, abas utilizadas para divulgação de atualizações da ferramenta, normas do TCMSP, *download* de aplicativos que dão suporte às atividades de instrução de processos, etc.

   - **Incluir opção para orientar os usuários do sistema sobre sua responsabilidade quanto aos registros, ao tratamento e à divulgação de dados sensíveis em conformidade com a LGPD.**

2. Cadastro de protocolos, recurso utilizado pela **UTPA** e também pelo **Portal do Jurisdicionado (avaliar solução do Portal individualmente).**

   a. Na tela de cadastro de protocolo, seja para expediente ou processo, o sistema permite selecionar a UG e Gestor correspondente, **exibindo nome, CPF e dados adicionais**.

   b. Ao confirmar o registro do protocolo, o sistema emite **Recibo de Protocolo** com os principais dados de classificação do registro.

   - **Inclusão de "texto" no Recibo de Protocolo** com orientações sobre LGPD e/ou;
   - Emissão de **Termo de Responsabilidade** junto com a emissão do Recibo de Protocolo.

3. Cadastro/Consulta de Pessoas registradas no e-TCM para associação a protocolos de processos ou expedientes.

a. A Consulta de “Pessoa” oferece opção de busca por **Nome e CPF** com opção de acesso ao Cadastro de “Pessoa” para **usuários autorizados (parametrização de perfil de usuário)**.

b. O Cadastro de Pessoas permite o registro de informações pessoais com identificação, endereço, contatos, inclusão de registro funcional e demais documentos necessários para identificação do individuo.

4. Cadastro de interessados, utilizado para vincular registro de pessoa ao registro de protocolo de processo ou expediente, permitindo a busca de registros de protocolos por nome ou CPF (busca mais exata).

a. O cadastro de interessados, vinculado ao registro de protocolo, exibe dados de identificação do individuo (pessoa física ou jurídica) e também sua classificação.

5. Avaliar necessidade de inclusão de “texto” com orientação sobre a LGPD em cada tela de recurso que trata dados sensíveis. Capa do processo

a. Apresenta os dados principais do processo e a relação de interessados por nome e CPF.

- A capa do processo é a primeira peça e pode ser concedida sua visualização através de consultas via Site do TCMSP ou pedidos de vistas. Sugere-se a exclusão do CPF e/ou qualquer outro dado referente a pessoa física ou jurídica que possa caracterizar informação sensível.
- O recurso **“Gerar um arquivo com todas as peças/ documentos”** da tela de visualização de detalhes do protocolo, gera um único arquivo PDF com todas as peças do processo, inclusive a capa, com tratamento de anonimização apenas para documentos

"desentranhados". O PDF gerado pelo recurso normalmente é utilizado para conceder vista ao processo (eletrônico).

6. Tela de visualização de peças e detalhes de protocolo
   a. Apresenta os dados de identificação dos interessados no andamento do processo ou expediente: nome, CPF e dados de classificação do tipo de interesse.
7. Consultas
   a. e-TCM
   b. Portal do TCM SP (*site*)
8. Portal do Jurisdicionado
9. Módulo Acesso à Informação para publicação de relatórios de fiscalização e outros
10. Sigilo de protocolos de processos, expedientes e peças especificas de protocolos
11. Papéis de trabalho anexados aos protocolos
12. Comunicações Processuais
13. Certidões
14. Relação de inelegíveis
15. Pedido de vistas de processo
16. Página no Portal do TCMSP específica para assuntos da LGPD

Ressalta-se, ainda, que as equipes de desenvolvimento (UTDS) e de suporte do e-TCM (NTI) já se reuniram para discutir sobre as adequações necessárias com objetivo de estimar tempo e recursos para as seguintes providências:

(a) Desenvolvimento de página *web* destinada à divulgação de informações e notícias relacionadas ao projeto de implantação da LGDP.

- O desenvolvimento pode ser iniciado a partir da definição do escopo da página, com especificação do conteúdo e responsável.
- O prazo para conclusão será estimado de acordo com o escopo e poderá ser concluído em curto prazo.

(b) Criação de espaço para exibição de mensagens de alerta nas telas do sistema onde há acesso a dados sensíveis.

- O desenvolvimento pode ser iniciado a partir da indicação das telas e principais recursos do e-TCM que deverão exibir as mensagens.
- O texto das mensagens deve ser encaminhado para a equipe de desenvolvimento e de acordo com cada tela selecionada para alteração.
- O prazo para conclusão será estimado de acordo com o escopo e poderá ser concluído em curto prazo.

(c) Emissão de Termos de Confidencialidade e controle de aceites

- Poderá ser implementado conforme identificação da necessidade de emissão de Termo e controle dos aceites ou negativas. O escopo deve ser definido pela equipe responsável e encaminhado para desenvolvimento, observando os pontos estratégicos de cadastro de dados e compartilhamento de documentos atendendo determinações.

- O prazo para conclusão será estimado de acordo com o escopo e poderá ser concluído em curto ou médio prazo.

(d) Implementação de melhorias para o requisito de gestão de sigilo de processos e documentos, com adequação dos demais recursos do sistema que estão integrados à gestão de sigilo, compartilhamento de documentos, consultas, etc.

- Revisão da Resolução 29/2019 e Portaria 05/2020 com inclusão de motivo para atribuição de acesso restrito a peça específica de processo ou expediente.
- Elaboração de manual de instruções.
- Treinamento dos usuários para uso dos novos recursos, descentralizando a gestão do sigilo que hoje é realizada exclusivamente pela equipe de Suporte e-TCM.
- O prazo para conclusão está estimado para dezembro/2020.

10. Providências urgentes a serem adotadas pelo TCMSP em decorrência do início da vigência da LGPD

- Criação de aba no *site* do TCM.

  Comentários:

  A *aba* deve conter as principais legislações referentes à LGPD e as providências que estão sendo adotadas no tocante à política de proteção

de dados do TCMSP. O desenvolvimento deverá ser feito pelo NTI com atuação deste grupo de trabalho quanto à inserção do conteúdo;

- Disponibilização imediata de canal (*e-mail* e telefone) para receber os requerimentos de terceiros[36].

  Comentários:

  Esse canal deve ser disponibilizado no *site* do TCMSP e, caso a opção seja pela utilização de área já existente no Tribunal, sugere-se a

[36]LGPD - Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e **mediante requisição**:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º **O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.**
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º **O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.**
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (grifos nossos).

Ouvidoria como responsável para receber as demandas inerentes à LGPD;

- Disponibilização no *site* do TCMSP de informação sobre a política de proteção de dados[37];

  Comentários:

  Em desenvolvimento

- Normatizar a regulamentação das atribuições do TCM como órgão controlador, com a indicação da estrutura funcional e das áreas envolvidas no tratamento de dados pessoais no âmbito do TCMSP.

  Comentários:

  Como sugestão, poderá ser nomeado uma Equipe de Gerenciamento da LGPD ou deixar a cargo da Presidência;

- Nomeação do encarregado.

  Comentários:

  Pode-se optar por mais de um encarregado, a exemplo do TJSP;

- Início da anonimização dos dados pessoais no processo eletrônico.

  Comentários:

  As providências inerentes à anonimização devem advir de trabalho em conjunto a ser realizado pelo encarregado (ou equipe) e pelo NTI;

[37] Como referência, cumpre citar o conteúdo trazido no site do TCE-SP, disponível em https://www.tce.sp.gov.br/politica-privacidade.

- Disponibilização no protocolo eletrônico do TCM de termo de aceite e de comunicado sobre a proteção de dados e de termo de aceite sobre eventuais dados pessoais e pessoais sensíveis.

  Comentários:

  Demanda parcialmente atendida em conjunto com o *Grupo de Intervenção do Portal do Jurisdicionado*;

- Disponibilização de termo de responsabilidade aos servidores para fins de acesso a dados pessoais e pessoais sensíveis;

- Disponibilização de termo de responsabilidade para fins de acesso a dados pessoais e pessoais sensíveis quando do pedido de vista dos autos.

11. Demais providências a serem adotadas

- Capacitação da estrutura funcional e das áreas envolvidas no tratamento de dados pessoais no âmbito do TCMSP;

- Capacitação dos demais servidores do Tribunal;

- Adaptação do Portal do Jurisdicionado, bem como de outras ferramentas de tecnologia a serem requisitadas pelo NTI;

- Adaptação das demais normas que possuem impacto com a política e tratamento de dados;

- Manutenção da *aba* do *site* da LGPD;

- Providências no sentido de acompanhar a atuação da Autoridade Nacional de Proteção de Dados em virtude de eventual necessidade de remessa do processo de implantação da LGPD no âmbito do TCMSP.

12. Dúvidas e Circunstâncias

Ainda em se considerando as conclusões alcançadas, há que se compreender, igualmente, as limitações e as potencialidades de que o TCMSP dispõe contemporaneamente para a concretização de eventuais ajustes.

Isto é, na gestão de quaisquer das etapas de tratamento de dados pessoais atualmente vigentes nos fluxos de trabalho das áreas do TCMSP, qual a extensão de que disporia o Tribunal de recursos materiais, técnicos e humanos para a realização *autônoma* – sem a inserção de terceiros – da adequação às medidas entendidas como necessárias?

O reconhecimento das alterações que se farão imprescindíveis – ainda internamente debatidas – passa direta e necessariamente pela apreciação do Núcleo responsável pela gestão dos recursos tecnológicos do TCMSP, particularmente relevante após a implementação do processamento eletrônico no ambiente virtual do Tribunal.

Tendo-se em vista o pragmatismo na implementação da norma, é fundamental que reconheçamos as possibilidades e as impossibilidades de concretização das medidas que o grupo entender cabíveis, à luz dos recursos humanos e técnicos de que dispõe o TCMSP.

São Paulo, 21 de setembro de 2020.

Unidade responsável: **Assessoria Jurídica de Controle Externo**

Patrocinadora: **Egle dos Santos Monteiro -** Assessora Jurídica Chefe de Controle Externo

Gerente do Projeto: **Maria Fernanda Pessatti de Toledo -** RF 1592

Equipe:

Diana Campos Dahdal (AJCE) – RF 20183

Valdir Godoi Buqui Netto (EGC) – RF 20295

Gisele dos Santos Venier (NTI) – RF 1619

Carlos Albuquerque Lemos (SFC) – RF 20289

Margarida Isabella Malena Mancini (SFC) – RF 741

Smara Gonsaga Silva (SG) – RF 840

George Augusto Niaradi (GAB-DD) – RF 1597

Sofia Bordin Rolim (GAB-MF) – RF 1615

Heraldo Brito da Silveira (GAB-ES) – RF 1501

Natália Schorr Carvalho Leme (GAB-JA) – RF 20105

Cintia Regina Beo (GAB-MF) – RF 1574

Alvaro Theodor Herman S. Caggiano (GAB-RB) – RF 1530