LGPD

Sugestões para a preparação da Diretoria de Informática do Tribunal de Justiça do Estado de Goiás para a entrada em vigência da Lei Geral de Proteção de Dados em maio de 2021.

MINUTA

07/07/2020

Lei Geral de Proteção de Dados Pessoais nº 13.709, conhecida pela sigla LGPD, promulgada em 14/8/18, sancionada em agosto de 2018 e começará a viger no dia 3/5/2021 (MP 959 - 29/04/20).

Engº Demetrius Jayme de Camargo
NSAD - Núcleo de Segurança e Administração de Dados
6433/D CREA-GO

Sumário

Anexo I

(Texto completo da LGPD)

Anexo II

(Texto completo da Medida Provisória nº 959 de 29/4/20)

Anexo III

(Guia de Boas Práticas LGPD - Governo Federal)

Anexo IV

(Relação de sistemas existentes no TJGO)

Anexo V

(Relação de sistemas existentes na Corregedoria Geral de Justiça)

Anexo VI

(Visita feita ao Conselho Nacional de Justiça)

Anexo VII

(Glossário LGPD)

Anexo VIII

(Decreto Judiciário nº 181/2020 - Criação do Comitê Gestor de Segurança da Informação)

Introdução

O objetivo deste estudo é deixar a *Diretoria de Informática (DI)* do *Tribunal de Justiça do Estado de Goiás (TJGO)* preparada para o início da vigência da nova lei em 3/05/2021. Não há aqui o propósito de se apresentar uma metodologia de implementação da *LGPD* ou abranger e esgotar todos os aspectos de tal lei, uma vez que algumas diretrizes de proteção de dados dela necessitam de detalhamento, em regulamentos e procedimentos próprios, a serem editados pela *Autoridade Nacional de Proteção de Dados (ANPD)* que ainda não se encontra em funcionamento.

Inicialmente, a adequação dos órgãos e entidades em relação à *LGPD* envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação envolve: considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (Privacidade by Design) e promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Cumpre destacar que o princípio da finalidade do tratamento de dados estabelecido na *LGPD* exige que os propósitos do tratamento sejam legítimos, específicos, explícitos e informados ao titular. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades. No caso do setor público, a finalidade relaciona-se com a execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador. O consentimento, quando exigido pelos órgãos públicos, será medida excepcional e deverá se referir a finalidades determinadas e comunicadas claramente ao titular do dado.

Conscientizar a alta gestão, definir o escopo, capacitar os colaboradores e efetuar um inventário de todos os dados devem ser elencados como as tarefas principais que o *Tribunal de Justiça do Estado de Goiás* deve realizar antes da vigência da nova lei em maio de 2021.

Estrutura da lei

Após o estudo e entendimento da nova lei pontuamos a seguir os pontos que consideramos mais relevantes dentro da realidade da *Diretoria de Informática* deste Tribunal.

A *Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n° 13.709/2018)* foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

Em 29/4/20 a *Medida Provisória nº 959* alterou o início da vigência da lei para o dia 3/5/2021.

Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

À seguir, são explicitados os principais conceitos da lei:

- **Dados pessoais**
  É uma informação que permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereços IP, cookies, etc.

- **Dados sensíveis**
  São dados sobre crianças, adolescentes, origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biomédicas e sobre a saúde ou vida sexual de uma pessoa.

- **Titular dos dados**
  Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. A *LGPD* permite ao titular acessar os seus dados a qualquer momento, conferindo se eles estão sendo tratados de alguma maneira. Também permite descobrir com quais instituições seus dados foram compartilhados, corrigir dados errados, atualizar outros que já expiraram, transferir os mesmos dados para outra entidade pública ou privada, deletar os dados que estão sendo tratados e até revogar o consentimento.

- **Consentimento dos dados**

  O titular dos dados deve se manifestar de maneira livre, informada e inequívoca pela qual concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O não consentimento é a exceção: só é possível processar dados, sem autorização do cidadão, quando isso for indispensável para cumprir situações legais previstas da *LGPD* e/ou em legislações anteriores.

  Por exemplo, uma organização - pública ou privada - pode, sem precisar pedir novo consentimento, tratar dados tornados anterior e manifestadamente públicos pelo cidadão.

- **Anonimização e pseudonimização**

  Dado anonimizado é aquele que, originalmente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Se um dado for anonimizado, então a LGPD não se aplicará a ele. É necessário frisar que um dado só é considerado efetivamente anonimizado se não permitir que, por meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará então sujeito à LGPD.

- **Tratamento dos dados**

Considera-se "tratamento de dados" qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essas operações de tratamento são destacadas a seguir:

Acesso - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

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 esgotado a sua vigência.

Avaliação - analisar o dado com o objetivo de produzir informação.

Classificação - maneira de ordenar os dados conforme algum critério estabelecido.

Coleta - recolhimento de dados com finalidade específica.

Comunicação - transmitir informações pertinentes a políticas de ação sobre os dados.

Controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado.

Difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados.

Distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido.

Eliminação - ato ou efeito de excluir ou destruir dado do repositório.

Extração - ato de copiar ou retirar dados do repositório em que se encontrava.

Modificação - ato ou efeito de alteração do dado.

Processamento - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado.

Produção - criação de bens e de serviços a partir do tratamento de dados.

Recepção - ato de receber os dados ao final da transmissão.

Reprodução - cópia de dado preexistente obtido por meio de qualquer processo.

Transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro.

Transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.

Utilização - ato ou efeito do aproveitamento dos dados. Ademais, é importante esclarecer que, por taxativa previsão da *LGPD (Art. 4°)*, as disposições da Lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos.

II - realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os *arts. 7º e 11 da LGPD*).

III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou.

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na *LGPD*.

Os casos de tratamento de dados que estão previstos e permitidos pela *LGPD* serão explicados a seguir. Mas é muito importante destacar que eles não são amplos e absolutos; ao contrário, existem limites para essa operação que estão dados pela boa-fé e demais princípios previstos no *Art. 6º* da mesma norma.

Antes de iniciar alguma espécie de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

O tratamento para cumprimento de obrigação legal ou regulatória pelo controlador também é uma hipótese corriqueira no serviço público. Nessas duas situações, o consentimento do titular de dados é dispensado.

Por outro lado, em hipóteses bastante específicas, o consentimento do titular pode ser necessário para finalidades determinadas. Quando isso ocorrer, as autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

Além disso, no tratamento feito pelo poder público, as regras previstas nos *artigos 23 (procedimentos de atuação)* e *30 (regulamentos da ANPD)* da *LGPD* sempre devem ser seguidas de forma complementar.

A *LGPD* previu expressamente em seu *artigo 7°*, dez hipóteses de tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.

Nesses casos, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados. É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência.

A *LGPD* especifica e regulamenta a função de três agentes principais:

- **O Controlador** é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do

tratamento de tais dados. No *Tribunal de Justiça do Estado de Santa Catarina* a figura do Controlador é o próprio Presidente do Tribunal.

- **O Operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

- **O Encarregado de dados** (ou **DPO - Data Protection Officer**) é a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional. É o responsável pela proteção dos dados na organização.

  Ao DPO cabem as seguintes tarefas:
  - Sensibilização e informação de todos que tratem dados pessoais.
  - Assegurar o comprimento das políticas de privacidade e proteção de dados.
  - Controlar e regular a conformidade da *LGPD*.
  - Recolher informação para identificar atividades de tratamento.
  - Controlar e acompanhar a produção do *RIPD – Relatório de Impacto sobre Proteção de Dados*.
  - Promover as abordagens de Privacidade por Desenho e por Padrão.
  - Realizar a avaliação na exposição aos riscos de violações de privacidade e mitigados com ações de melhoramento.
  - Recolher informação para identificar atividades de tratamento.
  - Manter atualizado os registros das atividades de tratamento de dados.
  - Controlar o cumprimento das cláusulas de proteção de dados junto aos fornecedores.
  - Promover formações de boas práticas para a proteção de dados.
  - Ser o ponto de contato com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados.
  - Ser o ponto de contato com as autoridades de controle.

O *Encarregado de dados* deve entender a visão estratégica do tratamento de dados pessoais pois, caso contrário, se torna um risco ético e de negócio para a instituição.

Além disso, sugerimos que seja subordinado ao *Comitê Gestor de Segurança e Informação (Decreto Judiciário n° 181/2020)* e exclusivo com a missão de proteger os dados e fazer cumprir a *LGPD* em toda a sua extensão na instituição.

Dessa maneira o *artigo 41* da *LGPD* rege as definições e atribuições do *encarregado de dados (DPO):*

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;

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."

- **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)**

Representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o *inciso XVII* do *art. 5º* da *LGPD*, o *RIPD* é documentação que deve ser mantida pelo Controlador dos dados pessoais.

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

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

Enquanto o *art. 5º inciso XVII* define o que é um *RIPD*, o seu conteúdo mínimo é indicado pelo parágrafo único do *art. 38*, grifado abaixo.

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.

- **Limitação da coleta**

A coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.

- **Minimização dos dados**

A coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.

- **Limitação de uso, retenção e divulgação**

O uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

- **Sanções para quem descumprir a lei**

A *LGPD* é uma lei que impõe sanções variadas a quem infringir as regras. Inicialmente é dada uma advertência simples, que determina uma data para correção da irregularidade.

Multas de até 2% do faturamento líquido da empresa também podem ser aplicadas, não chegando a mais de R$ 50 milhões, havendo a possibilidade também de aplicação de multa diária.

Outra forma de punição é a divulgação da irregularidade no tratamento de dados, tornando pública a infração caso seja confirmada após investigação. Da

mesma maneira, os dados pessoais podem ser bloqueados e até retirados do sistema da organização.

De acordo com o ranqueamento que poderá ser criado pelo CNJ (Conselho Nacional de Justiça) o Tribunal que acumular muitas reclamações, advertências e multas poderá ser rebaixado em sua escala de excelência.

- **Leis semelhantes no mundo**
    - **GDPR** - General Data Protection Regulation em vigência na comunidade européia.

    - **HIPAA** - Health Insurance Portability and Accountability Act em vigência nos Estados Unidos.

Sugestões de ações imediatas a serem tomadas

Os preparativos que antecedem a entrada em vigência da *LGPD,* para serem adotados, necessitam do amplo apoio da estrutura organizacional do *Tribunal de Justiça do Estado de Goiás*.

A *LGPD* é uma disrupção com a estrutura vigente. Por envolver uma mudança enorme no que tange à proteção dos dados pessoais será necessário envolver todos os nichos do *Poder Judiciário do Estado de Goiás* neste trabalho.

Unir as competências dos diversos setores existentes, tais como: jurídico, administrativo e técnico em um grupo de trabalho executivo aumenta consideravelmente as chances de sucesso dessa extensa empreitada: **Implantar a LGPD no âmbito do Tribunal de Justiça do Estado de Goiás.**

Visando preparar e aumentar a aderência da estrutura de software e hardware existente na *Diretoria de Informática (DI)* para receber a nova lei, sugerimos, salvo melhor juízo, a adoção e realização imediata das ações relacionadas abaixo:

N	Ação	Feito?
1	CRIAR um COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, conforme *artigo 9º* da *Resolução 211* de 15/12/2015 do CNJ (Solicitação já em andamento através do *PROAD nº 201908000184704*). Comitê criado no dia 28/01/2020, através do *Decreto Judiciário de n°181/2020*.	Sim
2	CRIAR UM GRUPO DE TRABALHO EXECUTIVO para elaborar os estudos de implantação da *LGPD* no âmbito do *Tribunal de Justiça do Estado de Goiás*. Esse grupo deverá ter em sua composição, além dos técnicos da área de *TI (Tecnologia da Informação)*, gestores das áreas envolvidas e consultores jurídicos que irão ajudar no sentido de adequar o *TJGO* às normas da lei. É de bom tom que o referido grupo possa contemplar visões múltiplas (área de processos, jurídica e tecnológica) em busca da conformidade e excelência.	Não

3	DEFINIR, através do grupo de trabalho, O ESCOPO DA APLICAÇÃO DA *LGPD* no âmbito do *Tribunal de Justiça do Estado de Goiás.*	Não
4	DEFINIR, através do grupo de trabalho, uma das figuras mais importantes da LGPD: O CONTROLADOR. Responsável pela gestão é também o guardião maior em relação a lei. No *Tribunal de Justiça do Estado de Santa Catarina* a figura do Controlador é o próprio Presidente do Tribunal.	Não
5	DEFINIR, através do grupo de trabalho, O OPERADOR.	Não
6	DEFINIR, através do grupo de trabalho, o ENCARREGADO DOS DADOS ou DPO (DATA PROTECTION OFFICER).	Não
7	EFETUAR uma AUDITORIA completa em TODOS OS SISTEMAS EXISTENTES no TJGO (ver lista no ANEXO IV) para verificar se todos eles são aderentes à aplicação da nova lei ou se necessitam de modificações. A lista existente deverá ser validada pela área de desenvolvimento de software responsável que deverá relacionar apenas os sistemas que estão efetivamente em uso. Os demais sistemas que deixaram de ser utilizados deverão ser bloqueados para uso. Os dados pessoais que forem encontrados nesta auditoria deverão ser reanalisados de modo a verificar se poderão passar por um processo de minimização, anonimização ou pseudonimização.	Não
8	EFETUAR uma AUDITORIA completa em TODOS OS SISTEMAS EXISTENTES na CORREGEDORIA GERAL DE JUSTIÇA em funcionamento (ver lista no ANEXO V) para verificar se todos eles são aderentes à aplicação da nova lei ou se necessitam de modificações. A lista existente deverá ser validada pela área de desenvolvimento de software responsável que deverá relacionar apenas os sistemas que estão efetivamente em uso. Os demais sistemas que deixaram de ser utilizados deverão ser bloqueados para uso. Os dados pessoais que forem encontrados nesta auditoria deverão ser reanalisados de modo a verificar se poderão passar por um processo de minimização, anonimização ou pseudonimização.	Não
9	MONTAR UMA ESTRUTURA PARA DAR APOIO AO TITULAR DOS DADOS caso sejam encontrados dados pessoais sensíveis após a realização da auditoria sugerida. Essa estrutura deverá permitir:	Não

	- Solicitar o consentimento do titular dos dados para tratá-los e/ou usá-los com um fim específico. - Deverá ser capaz, se solicitada, de fornecer ao titular dos dados todas as informações armazenadas na organização em seu nome. - Informar ao titular dos dados se houver algum incidente de segurança.	
10	ANALISAR A INFRA-ESTRUTURA COMPUTACIONAL EXISTENTE visando minimizar os riscos de possíveis vazamentos de dados dotando-a dos recursos tecnológicos mais modernos.	Não
11	APÓS A IMPLANTAÇÃO DA LGPD NO ÂMBITO DO TJGO E NO INTUITO DE PRESERVAR TODO O TRABALHO JÁ REALIZADO, o grupo de trabalho criado, deverá ser o ente responsável, dentro do TJGO, para verificar e autorizar a criação e/ou alteração de novas rotinas, processos, programas, softwares, apps, relatórios, publicações em redes sociais, etc.	Não
12	REALIZAR AUDITORIA PARA VERIFICAR SE SISTEMAS DESENVOLVIDOS EM OUTROS ÓRGÃOS do Estado ou município, mas que têm permissão para acessar os bancos de dados próprios do TJGO, terão algum impacto após a nova lei entrar em vigor.	Não
13	REALIZAR AUDITORIA PARA VERIFICAR COMO PRINTS DE TELAS E RELATÓRIOS, autorizados ou não pelos usuários dos sistemas do TJGO, terão algum impacto após a nova lei entrar em vigor.	Não
14	REFORÇAR A POLÍTICA DE SEGURANÇA JUNTO AOS USUÁRIOS no intuito de evitar a ocorrência de senhas ‘consideradas fracas’ que possam ser facilmente descobertas e utilizadas de modo criminoso no intuito de vazar dados pessoais não autorizados.	Não
15	REALIZAR AUDITORIA NO SENTIDO DE LEVANTAR POSSÍVEIS USUÁRIOS, que apesar de não terem mais acesso por algum motivo (aposentadoria ou mudança de função) continuam acessando dados pessoais relevantes.	Não
16	REALIZAR AUDITORIA NO SENTIDO DE VERIFICAR COMO PROTEGER os DADOS que estão PRESENTES EM MEIOS FÍSICOS tais comos: papéis e outros.	Não

Matriz SWOT

Para se implantar uma lei tão abrangente e complexa é necessário avaliar as considerações da Matriz SWOT abaixo:

Forças *(Strengts) Vantagens internas da instituição*

- Grande comprometimento dos magistrados e servidores no cumprimento do trabalho a eles designado.
- Boas práticas desenvolvidas e adotadas por magistrados e servidores.
- Forte atuação dos Comitês Gestores do *TJGO*.

Fraquezas *(Weakness) Desvantagens internas da instituição*

- Necessidade de informar e treinar todos os magistrados e servidores no manejo eficiente da nova lei.
- Possível falta de recursos financeiros frente à Pandemia do Covid-19.
- Extenso trabalho a ser feito nas auditorias no acervo de dados existente.

Oportunidades *(Opportunities) Aspectos positivos do ambiente que envolve a instituição com potencial de trazer-lhe vantagem competitiva*

- O Titular dos dados pode conceder o acesso aos seus dados de maneira total ou parcialmente. É possível obter um retorno financeiro desta concessão (vide exemplo do plano de saúde).

- Possibilidade do *TJGO* se elevar no ranking atual do *CNJ* e conquistar novas menções e prêmios se sair à frente de outros tribunais na implantação da nova lei.

Ameaças *(Threats) Aspectos negativos do ambiente que envolve a instituição com potencial para comprometer a sua vantagem competitiva*

- Como a pandemia do Covid-19 vai impactar em todo o processo?
- A LGPD vai entrar em vigor em maio de 2021 mesmo? Não será adiada novamente?

- A *PEC nº 17/2019* que incluir a proteção de dados pessoais físicos e digitais entre os direitos e garantias fundamentais do cidadão brasileiro vai ser aprovada mesmo?
- Quando a *ANPD - Agência Nacional de Proteção aos Dados* será criada efetivamente?

Conclusão

Apesar da entrada em vigência da nova lei ter sido adiada para maio de 2021, os Tribunais, até lá terão que realizar um trabalho hercúleo para adequar a sua estrutura e processos atuais à nova realidade.

A proteção dos dados pessoais, à partir desta data elevará direitos e obrigações civis à patamares nunca antes alcançados.

Processos e sanções frutos de possíveis vazamentos de dados pessoais, serão cada vez mais comuns nesse novo mundo que se configura, exigindo do ente público um cuidado e zelo maior com as informações ali depositadas.

Cada vez mais exigidos pelo *Conselho Nacional de Justiça* e pela sociedade em geral, os Tribunais Estaduais que pretenderem se sobressair em um futuro próximo, deverão iniciar os preparativos de adequação à nova lei o mais breve possível.

Dentro do rol das ações elencadas em nosso estudo estão algumas que, para agilizar o processo, poderão ser contratadas no mercado de serviços e soluções de TI tradicional.

Em visita ao *CNJ (Conselho Nacional de Justiça)* no dia 11 de março do corrente ano fomos informados, em caráter não oficial, que o Conselho deve prestar orientações para nortear a implantação da *LGPD* pelos Tribunais Estaduais.

Sugerimos, salvo melhor juízo, que este estudo deve ser analisado, discutido e alterado (se for o caso) pelo corpo executivo da *Diretoria de Informática (DI)* e pelos integrantes deste *Núcleo de Segurança e Administração de Dados (NSAD)*. Após, sugerimos a criação de um processo PROAD a ser encaminhado à *Comissão de Informatização* e ao *Comitê Gestor de Segurança da Informação* recém criado para deliberações pertinentes.

Bibliografia

Sítio da Presidência da República do Brasil
Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD)
http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Sítio do Conselho Nacional de Justiça - CNJ
https://www.cnj.jus.br/

Sítio do Serviço Federal de Processamento de Dados - SERPRO
https://www.serpro.gov.br/lgpd

Sítio da Associação Brasileira de Defesa do Consumidor
PROTESTE
https://www.proteste.org.br/

Sítio da Escola Nacional de Administração Pública - ENAP
https://www.enap.gov.br/pt/

Sítio da Câmara dos Deputados
https://www.camara.leg.br/

Sítio do Governo Federal
Guia de Boas Práticas (LGPD)
https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf

Medida Provisória nº 959 de 29/04/2020
http://www.in.gov.br/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639?inheritRedirect=true&redirect=%2Fweb%2Fguest%2Fsearch%3FqSearch%3Dmedida%2520provis%25C3%25B3ria%2520959

Sítio do Tribunal de Justiça do Estado de Santa Catarina
(Criação do Comitê Gestor de Proteção de Dados)
https://www.tjsc.jus.br/comite-gestor-de-protecao-de-dados?inheritRedirect=true

ANEXO I

(Texto completo da LGPD)

ANEXO II

(Texto da Medida Provisória nº 959 que adiou a LGPD)

ANEXO III

(Guia de Boas Práticas da LGPD)

ANEXO IV

(Relação de Sistemas do TJGO)

Sistemas existentes:

- PROJUDI
- PJD
- PJE
- PROAD - PROCESSO ADMINISTRATIVO DIGITAL
- ARCA
- PGWEB - FOLHA DE PAGAMENTO
- SISTEMA DE ARRECADAÇÃO
- CENTRAL DE MANDADOS
- ESCRIVANIAS CRIMINAIS (NATURAL/ADABAS)
- EXECPENWEB
- EXECPEN
- AGENDA ELETRÔNICA DO TELEJUDICIÁRIO
- SISTEMA DE BIBLIOTECA
- CONTROLE DE BENS
- CONTROLE DE ESTACIONAMENTO
- CVJ - CADASTRO DE VITIMAS DO JUIZADO DA MULHER
- CONTEC - CONTROLE DE EXPEDIENTE CRIMINAL
- CURSOS - CAPACITAÇÃO E DESENVOLVIMENTO
- FUNDO ROTATIVO
- GPWEB - SISTEMA DE GESTÃO DE PROJETOS
- MALOTE DIGITAL
- OMD - SISTEMA INFORMATIZADO PARA GESTAO DE OUVIDORIAS
- PORTAL DE ESTRATÉGIAS TJGO
- OCOMON - SISTEMA DE MONITORAMENTO DE OCORRÊNCIAS
- RSO - REGISTRO DE SUSTENTAÇÃO ORAL
- SAP - SISTEMA DE ACOMPANHAMENTO PROCESSUAL (CNJ)
- SIGA - SISTEMA INTEGRADO DE GESTÃO ADMINISTRATIVA
- SISCON - SISTEMA DE CONTRATOS
- SOF - SISTEMA ORÇAMENTÁRIO FINANCEIRO
- SPCOM - SISTEMA DO PERFIL DAS COMARCAS
- SCF - SISTEMA DE CADASTRO DE FORNECEDORES

- SPE - SISTEMA DE PONTO ELETRÔNICO
- SIPEMA - SISTEMA DE PENAS E MEDIDAS ALTERNATIVAS
- SISTEMA DE CONCILIAÇÃO
- SCJ - CÁLCULO JUDICIAL
- SCP - SISTEMA DE CONTROLE DE POSTAGEM
- SEC - SISTEMA DE ESTATÍSTICA DA CORREGEDORIA
- TJDOCS - SISTEMA DE DESPACHOS E ATOS ADMINISTRATIVOS E JUDICIAIS
- WPRO - SISTEMA DE PROJETOS
- SGO - SISTEMA DE GERENCIAMENTO DE OBRAS

ANEXO V

(Relação de Sistemas Corregedoria de Justiça do TJGO)

Sistemas existentes:

- CONTROLE DO PRIMEIRO GRAU
- CONTROLE TURMA
- CONTROLE INTERPROFISSIONAL FORENSE
- CONTROLE EXTRAJUDICIAL
- PLANEJAMENTO E PROGRAMAS
- GESTÃO SEM DISTÂNCIA
- CONTROLE DE PERITOS
- CONTROLE DE ADMINISTRADORES JUDICIAIS

ANEXO VI

(Visita feita ao Conselho Nacional de Justiça - CNJ)

ANEXO VII

(Glossário LGPD)

ANEXO VIII

(Decreto Judiciário nº 181/2020 - Criação do Comitê Gestor de Segurança da Informação)