IOB, uma marca ao³

apresenta

Como está seu escritório contábil em relação à

Lei Geral de Proteção de Dados Pessoais

O e-book completo do workshop prático, apresentado por Juliane Borsato coordenadora de privacidade na ao³

Material produzido em maio/2021

E aí, empreendedor!

Em um mundo em que nossos dados valem ouro para os mais variados tipos de empresas, a necessidade de uma **regulamentação na coleta, armazenamento, tratamento e compartilhamento das informações** vem tomando o holofote nas discussões de diversos países ao redor do mundo.

Em agosto de 2018, o Brasil entrou na lista das nações que criaram iniciativas legais para garantir a privacidade de dados em seu território.

Com o prazo final de adaptação dado às empresas e organizações em terras brasileiras chegando, é necessário ter certeza que você e seu escritório estejam completamente por dentro da Lei Geral de Proteção de Dados Pessoais.

Entenda um pouco mais sobre a lei, obtenha orientações práticas para **aumentar seu conhecimento** sobre o assunto e tire suas principais dúvidas neste material feito pela ao³ **especialmente para você**.

Vamos lá? Boa leitura.

AVISO:

Todas as dicas e/ou orientações de processos oferecidas neste material têm o **objetivo de ensinar, inspirar e facilitar o processo de adequação** à LGPD. **As sugestões levantadas aqui devem ser validadas e acompanhadas pela área jurídica e técnica da empresa,** pois cada uma tem suas particularidades — o que leva à necessidade de adaptar as estratégias de acordo com o contexto e o perfil do negócio.

Assim nasce o direito à proteção de dados pessoais...

@ Por que a privacidade e proteção de dados é tão importante?

Para entrarmos de cabeça na **Lei Geral de Proteção de Dados Pessoais**, precisamos entender seus fundamentos. É na importância da privacidade e da proteção dessas informações que toda essa história começa.

A cada ano, as discussões envolvendo esses dois conceitos têm ganhado cada vez mais espaço e força. Com a ascensão da economia digital, uma quantidade gigantesca de dados é criada diariamente — e com grandes volumes de dados vêm grandes responsabilidades. Aqui entra a **proteção**, que é o meio para implementar o direito à **privacidade**, e a privacidade em si, que é o direito puro de ser protegido de qualquer interferência em assuntos pessoais.

Hoje, as informações pessoais são um recurso extremamente valioso para as instituições e empresas ao redor do mundo; — assim como para a economia em si, pois quando aliadas aos dados corretos e usadas de forma adequada, as informações pessoais trazem conhecimento ao seu detentor e ajudam na tomada de decisões importantes. É como o The Economist disse em uma publicação de 2017:

"The world's most valuable resource is no longer oil, but data."
"O recurso mais valioso do mundo não é mais o petróleo, mas sim os dados."

@ Origem da privacidade

O conceito de privacidade é **mais antigo do que você imagina**. Ele não surgiu com a criação da Internet, mas sim **décadas antes desse acontecimento.**

O ano é 1890

O começo simbólico de toda a ideia aconteceu a partir de um trabalho publicado na **Harvard Law Review**, cujo nome é **“The right to privacy”** — ou **“O direito à privacidade”**, em português — e tem como autores os advogados americanos Samuel Warren e Louis Brandeis.

Nesse ensaio, Warren e Brandeis analisam casos judiciais envolvendo propriedade, direitos autorais e difamação e, após todo esse estudo, elaboram o primeiro real significado do “direito de ser deixado em paz”. E não para por aí: eles advertem os leitores sobre os riscos que o surgimento de novas tecnologias e invenções traria à privacidade em si. Detalhe: **tudo isso lá no século 19!**

O artigo estava tão bem embasado que, em 1920, se tornou parte da Constituição norte-americana.

Em pouquíssimas palavras, a privacidade é o direito dado ao indivíduo de ter a garantia de controle sobre sua vida privada.

@ Chegando na Lei Geral de Proteção de Dados Pessoais

Em agosto de 2018, após a unificação dos textos da Câmara e do Senado, foi sancionada a Lei Geral de Proteção de Dados no Brasil. Meses depois, por meio da Medida Provisória nº 869, a Autoridade Nacional de Proteção de Dados (ANPD) foi criada. Finalmente, no dia 18 de setembro de 2020, a Lei nº 13.709/2018, também conhecida como LGPD, entrou em vigor em todo o território nacional.

@ Resumindo

Composta por 10 capítulos principais e 65 artigos, a LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade de cada pessoa dentro do território brasileiro. Ela conta com textos detalhados sobre sua definição e como ela deve ser aplicada (art. 1º a 5º); qual o modo correto de fazer a coleta e o tratamento das informações pessoais (art. 5º a 11, 15, 16 e 23); quais são os direitos do titular (art. 17 a 22); como pode ser feito o uso desses dados pelo poder público e a transferência internacional dessas informações; quem são as pessoas que podem fazer o tratamento das mesmas; segurança e boas práticas (art. 46 a 51); e como acontecerá e quem exatamente fará a fiscalização — com a definição do que é a ANPD e o que ela faz.

@ Para deixar a lei mais visual, os principais pontos são os seguintes:

Parte 1 - Proteção de Dados x Privacidade:	nenhum artigo específico
Parte 2 - O que é LGPD?	**LGPD:** art. 1
Parte 3 - Fundamentos e Escopo	**LGPD:** art. 2, 3 e 4
Parte 4 - Conceitos Chave	**LGPD:** art. 5
Parte 5 - Dados Pessoais	**LGPD:** art. 5, 11, 14
Parte 6 - Anonimização e Pseudonimização	**LGPD:** art. 5, 12
Parte 7 - Tratamentos de Dados Pessoais	**LGPD:** art. 5, 9
Parte 8 - Princípios	**LGPD:** art. 6
Parte 9 - Hipóteses Legais para Tratamentos	**LGPD:** art. 7, 11 e 23
Parte 10 - Consentimento e Legítimo Interesse	**LGPD:** art, 8 e 10
Parte 11 - Término do Tratamento	**LGPD:** art. 15, 16
Parte 12 - Direitos do Titular	**LGPD:** art. 17, 18, 19
Parte 13 - Papéis	**LGPD:** art. 37, 38, 39, 40, 41
Parte 14 - Responsabilidade e Penalizações	**LGPD:** art. 42 a 45 - 52 a 54
Parte 15 - Segurança Boas Práticas	**LGPD:** art. 46 a 51

@ Os riscos de não estar em conformidade com a LGPD

Falamos no início deste material sobre as responsabilidades, cada vez maiores, que temos em cima dos dados produzidos e coletados. Aqui,no artigo 42, abordamos isso com maior ênfase.

A lei é bem clara sobre o que acontece com o controlador ou o operador (ou seja, a empresa que faz a captação e/ou o tratamento dos dados) que causar algum dano, seja ele patrimonial, moral, individual ou coletivo, durante o processo de tratamento dessas informações: o responsável deverá reparar legalmente o indivíduo lesado. — o que poderá ser feito tanto por meio de indenização, quanto prestando solidariedade ao titular.

O artigo 52, traz 6 diferentes sanções e penalidades aos agentes que cometerem qualquer infração à lei. **A seguir, apresentamos três exemplos:**

Multa de até **2% do faturamento**, com limite de até R$ 50 milhões por infração.

A ANPD pode **bloquear** e/ou **eliminar** os dados.

A ANPD pode **suspender** ou **proibir** as atividades de coleta e tratamento de dados.

@ E se houver um caso de vazamento de informações?

Outra sanção, também citada no artigo 52, aplicável aos profissionais e às empresas que se envolverem em um incidente com dados pessoais,diz respeito à divulgação de dados ao público. Esse tipo de sanção será aplicada depois do vazamento ter sido devidamente apurado e confirmado pela ANPD, o que pode trazer efeitos irreversíveis à imagem do controlador ou operador.

LGPD: uma aliada de profissionais e negócios

Com os padrões técnicos de boas práticas definidos pela lei, a LGPD não veio barrar a evolução das empresas, mas sim ajudá-las a achar o modo mais correto de lidar com as informações, a expandir e oferecer melhores produtos e serviços e a proteger tanto o negócio como seu público. Na verdade, ela traz benefícios excelentes! Alguns exemplos:

PROTEÇÃO E SEGURANÇA:
Como citado anteriormente, o dado é um item valiosíssimo nos dias de hoje. A LGPD foi criada para proteger os ativos de informações da empresa, garantindo a continuidade do negócio e auxiliando na redução de possíveis danos e prejuízos.

MAIS CONFIANÇA E CREDIBILIDADE:
Ao estar em conformidade com a lei, a confiança por parte dos clientes e parceiros para com a empresa aumenta e muito! Além disso, a reputação e a imagem também melhoram aos olhos do mercado, transformando o comprometimento e o respeito à lei e aos usuários em um diferencial competitivo.

MAIS OPORTUNIDADES:
Os itens anteriores resultam neste terceiro. Isso porque o compromisso com a segurança das informações da empresa e a busca pela excelência e credibilidade perante os clientes criam o terreno perfeito para o fortalecimento de relações comerciais já existentes e novas oportunidades de negócios.

ACIMA DE TUDO:
A empresa estará de acordo com a lei, que já está em vigor e deve ser cumprida.

QUER TER CERTEZA DE QUE ESTÁ EM CONFORMIDADE COM A LGPD?

Acesse nossa avaliação* para saber, a partir de uma visão geral, se seu escritório ou sua empresa está de acordo com a Lei Geral de Proteção de Dados Pessoais! É gratuita:

Faça já sua avaliação

*Esta avaliação é apenas uma sugestão de plano de ação, com o objetivo de esclarecer dúvidas e oferecer insights, e não abrange todas as atividades necessárias. Observe suas particularidades e converse com suas áreas jurídica e técnica para validar o que é o melhor para seu escritório ou empresa.

LGPD na prática:

Ficando em conformidade com a lei

Fazer a adequação de escritórios ou empresas à LGPD não é algo rápido ou que se resolva apenas inserindo novas medidas de segurança ou mudando algumas regras. Para esse processo dar certo, é necessário o **comprometimento** e a **conscientização**de todos os profissionais envolvidos, além da elaboração, manutenção e revisão de documentos e processos.

É preciso que a LGPD vire uma cultura do dia a dia.

Escolha um método que **melhor se adeque** às particularidades de sua organização.

Comece devagar, por pequenos passos, criando um time ou um comitê especializado.

Entenda em que estágio de **maturidade** sua empresa está com relação à LGPD.

Peça **ajuda** quando não souber o que fazer ou por onde começar.

A Jornada de Adequação

Esse procedimento é muito importante, pois cria um conjunto de ações, de acordo com certa metodologia, que tornam o processo mais prático e permitem que a organização fique em conformidade com as legislações.

@ Primeiro passo: estabeleça uma metodologia

Definir uma metodologia ou um framework a ser seguido é essencial para a jornada de adequação. Ela deve ser selecionada com cuidado, de acordo com o contexto de cada empresa. O exemplo que traremos para você é um tipo de metodologia muito utilizada e que foi adaptada por John Kyriazoglou: o **SGPD — Sistema de Gestão de Proteção de Dados**.

SGPD → Um framework internacional e maduro que busca dar suporte e orientações em um projeto de adequação. Reconhecido na Europa e usado para o GDPR (Regulamento Geral de Proteção de Dados), ele traz uma metodologia consolidada em etapas, políticas, procedimentos e várias ferramentas técnicas, que auxiliam no suporte durante o processo de PD&P — Proteção de Dados e Privacidade. Ele é composto por cinco fases:

1ª - PREPARAÇÃO

Nesta etapa, é necessário fazer uma análise da privacidade: entender quais leis são pertinentes para seu negócio, conhecer e mapear o fluxo de dados de sua empresa, criar um programa de proteção de dados e privacidade e um plano de implementação.

2ª - ORGANIZAÇÃO

Aqui surge a criação de programas e políticas de controle para dar continuidade à PD&P: é necessária a criação de um canal interno de comunicação, que deve incluir a direção, além da implementação de sistemas informatizados para a sustentação da PD&P.

3ª - DESENVOLVIMENTO E IMPLEMENTAÇÃO

Momento de colocar em prática os planos e políticas, fazer a aprovação dos processamentos de dados pessoais e o registro dos bancos de dados, oferecer treinamentos e atividades de integração e fazer o controle de segurança.

4ª - GOVERNANÇA

Hora de implementar práticas de segurança, fazer planos de solicitações, reclamações e retificações, além de simulações de incidentes de privacidade.

5ª - AVALIAÇÃO E MELHORIA

Por último, é preciso analisar os relatórios de auditoria, o DPIA — ou Relatório de Impacto à Proteção de Dados — e as avaliações de benchmarks, monitorar as leis e regulamentos de Proteção de Dados e criar o programa de privacidade DPIA.

Desenvolvendo um Plano de Adequação

@ O começo

Existem muitos pontos importantes para fazer desse processo um sucesso. Alguns já citamos aqui, outros vão depender de detalhes específicos sobre seu negócio, da metodologia usada e de insights que você pode ter conversando com os profissionais das áreas jurídica e técnica. De uma forma ou de outra, existem quatro pontos principais aos quais você pode se atentar, confira:

PESSOAS

Atribua cargos e responsabilidades para profissionais envolvidos no processo de coleta e tratamento de dados; garanta o treinamento, a conscientização e a capacitação adequada a eles.

DADOS

Proteja seus dados. Defina o que são dados pessoais e sensíveis e o ciclo de vida de cada informação — ou seja, o dado foi coletado, tratado, utilizado para sua finalidade e agora é importante decidir o que fazer com ele: se será eliminado ou guardado.

TECNOLOGIAS

Defina quais são as tecnologias envolvidas: quais ferramentas serão usadas para promover a segurança e gerir os dados coletados, além de padrões e políticas (como Normas ISO, Privacy by Design etc.).

PROCESSOS

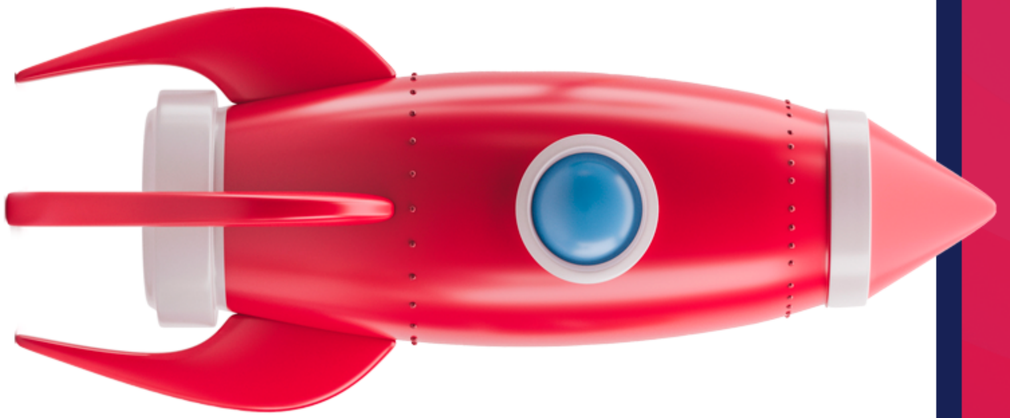
Estabeleça quais serão os processos de governança, gestão, monitoramento e melhoria contínua para seu negócio perante a lei.

@ As boas práticas são a alma do negócio

Confira algumas referências que você pode consultar para desenvolver boas práticas e, consequentemente, atingir **ótimos níveis de conformidade.**

O artigo **50 da própria Lei nº13.709/18**, que explica em detalhes as regras a serem seguidas para uma adequação ideal.	**A GDPR** — Regulamento Europeu nº 2016/679	**ISO 27001** — Sistema de Gestão de Segurança da Informação (SGSI)
ISO 27701 — Sistema de Gestão de Privacidade da Informação (SGPI)	**OWASP Top 10** — Medidas de Segurança	**NIST** (Instituto Nacional de Padrões e Tecnologia)
PCI (Payment Credit Industry) — para o financeiro		

@ Colocando seu plano em prática



Agora que você conhece todo o cenário e entendeu os passos anteriores, chegou o momento de colocar sua estratégia de implantação em ação. Alguns desses passos você já viu em itens anteriores, **mas é importante reforçá-los, agora, de maneira prática.**

PASSO 1:
COMITÊ

Forme um comitê com representantes de áreas - chave de seu negócio (como TI, RH, Marketing, Jurídico etc), entenda como cada uma delas pode contribuir e delegue a responsabilidade do mapeamento de dados ao profissional certo.

PASSO 2:
LGPD ASSESSMENT

Mapeie todos os dados, apresente os pareceres técnicos e jurídicos, entenda a maturidade de cada área perante a LGPD e o fluxo de informações e faça um planejamento sólido.

PASSO 3:
CAPACITAÇÃO

Realize treinamentos de capacitação, leve conhecimento a todos os profissionais e engaje a mudança da cultura interna de sua empresa.

PASSO 4:
CONTROLES

Execute o que até agora está no papel, faça os ajustes necessários na governança, nos processos e nas ferramentas.

PASSO 5:
CONFORMIDADE

Mantenha uma periodicidade nas avaliações e análises para permanecer em conformidade com a lei.

@ Dica para acelerar levemente o processo

A maior e principal orientação é contar com o auxílio da área jurídica para saber quais normas vão apoiar digitalmente e quais tecnologias de Recursos Humanos você precisará adotar. Além disso, é preciso conhecer muito bem as particularidades de seu negócio para escolher as estratégias e as ferramentas certas.

Se houver a necessidade de um empurrãozinho mais certeiro, enumeramos 4 exemplos de ações prioritárias que você pode tomar para acelerar um pouco o processo. São elas: nomear um DPO (art. 41), responder aos titulares (art. 18), implementar medidas de segurança técnicas e administrativas (art. 46) e alinhar a governança (art. 50). A seguir, destacamos duas delas:

NOMEIE UM DPO
Segundo o artigo 41, o controlador deverá indicar um encarregado para o tratamento de dados pessoais. Esse cargo pode ser ocupado por uma pessoa física, uma empresa ou escritório especializado.

A identidade desse profissional — ou empresa/escritório — e as informações para contato do mesmo devem ser divulgadas publicamente, de forma clara e objetiva (de preferência no site de sua empresa).

RESPONDA AOS TITULARES
Esse ponto tem muito a ver com o primeiro. Aqui, é importante que exista uma área para responder aos direitos dos titulares.

Segundo o artigo 18, os titulares podem requisitar o acesso aos dados que foram coletados sobre eles, a correção de informações incompletas, a anonimização, o bloqueio, a eliminação ou mesmo a portabilidade de algum dado etc. Por isso, há a necessidade de uma área dedicada a atender às necessidades do titular.

@ Um check-list para guiar você

Criamos uma lista com informações completas para te ajudar a não se perder no meio do processo. Basta acessar o arquivo, imprimir e dar “check” nos itens que você já realizou.

Clique aqui para baixar o arquivo da check-list.

Encontre a resposta de sua dúvida aqui

Durante o workshop, pedimos que você enviasse sua pergunta e prometemos disponibilizar a resposta posteriormente. Então aqui está!
Confira as principais dúvidas levantadas durante o evento:

1 - Minha dúvida é se vocês têm um modelo de cláusula para incluirmos em nosso contrato de prestação de serviços para a adaptação à LGPD e o que teremos que fazer com os funcionários de nossos clientes para termos acesso a suas informações pessoais.

Resposta: Há vários modelos de cláusulas para contratos de prestação de serviços, não existe um padrão pré-formatado. Esse tipo de documento deve ser analisado e construído pela área jurídica caso a caso, levando em consideração a situação fática e como será a aplicação da LGPD, de acordo com o tipo de prestação de serviços que está sendo realizada e quais dados serão coletados.

Dessa forma para a elaboração de um contrato de prestação de serviços que cumpra as normas LGPD, primeiro será preciso definir os papéis de cada um n a prestação de serviços, quem será o controlador e/ou operador dos dados e definir as responsabilidades de cada um no tratamento dos dados pessoais.

Uma vez estabelecido isso em instrumento contratual, haverá base legal para o tratamento dos dados dos funcionários de seus clientes conforme previsto no art. 7, inciso V da LGPD.

2 - No registro de funcionário, a empresa necessita de autorização para colher os dados obrigatórios da legislação trabalhista?

Resposta: Essa análise depende de quais dados estão sendo coletados. Por exemplo, o preenchimento de uma ficha ou do Livro Registro de Empregado com os dados do funcionário é uma exigência legal imposta ao empregador (artigos 41 a 48 da CLT). Dessa forma, a coleta desses dados possui base legal prevista no Art. 7, inciso II da LGPD fundamentando a necessidade de tratamento em decorrência de obrigação legal ou regulatória e dispensando a necessidade de consentimento, que também é uma base legal prevista no Art. 7 da LGPD, inciso I.

Deve-se levar em conta nas análises o Princípio da Necessidade que estipula dentro da LGPD que a coleta de dados deve se dar de maneira restritiva, prezando pelo tratamento de dados pessoais estritamente necessários ao atendimento da finalidade pretendida de forma proporcional, dispensando a coleta excessiva.

3 - Todo escritório é obrigado a ter um DPO, mesmo que não tenha colaborador?

Resposta: Sim. O artigo 41 da LGPD fala que toda empresa que desempenha alguma atividade em qualquer parte do processo de tratamento de dados deve ter um encarregado de proteção de dados (DPO). A única exceção está prevista no § 3º do art. 41 que dispõe sobre a possibilidade da ANPD dispensar a indicação do encarregado, a depender da natureza e porte da empresa, bem como o volume de dados tratados.

Ressalta-se que até o momento desta publicação **(11/06/2021)** não houve nenhum posicionamento da ANPD a esse respeito.

Ao definir o encarregado de proteção de dados (DPO) de sua empresa, é preciso identificá-lo e deixar as formas de contato divulgadas publicamente, de forma clara e objetiva, mesmo que a empresa não tenha colaboradores.

4 - Em relação à LPGD, como será o vínculo da ao[3] com o escritório?

Resposta: Gostaríamos de apresentar nossa Política de Privacidade que pode ser acessada no endereço https://info.ao3tech.com/politica-de-privacidade
No documento, reunimos alguns pontos importantes e comentamos sobre a relação entre a ao3 e o escritório:

- **Agente de tratamento dos dados**: ao3

- **Papel da ao3 no tratamento de dados:** Controlador. A depender da situação poderá ser operador ou controlador conjunto.

- **Informações pessoais coletadas:** Varia segundo o serviço prestado ao cliente

5 - Já foi constituída a ANPD (Autoridade Nacional de Proteção de Dados)?

Resposta: A ANPD foi criada pela Medida Provisória n. 869, de 27 de dezembro de 2018, posteriormente convertida na Lei n. 13.853, de 14 de agosto de 2019.

Por sua vez, o Decreto 10.474, de 26 de agosto de 2020, aprovou a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da ANPD, com entrada em vigor na data de publicação da nomeação do diretor-presidente da ANPD no Diário Oficial da União.

Em outubro de 2020, o Presidente da República Jair Bolsonaro indicou cinco nomes para o Conselho Diretor, órgão máximo da ANPD. Coronel Waldemar Gonçalves Ortunho Junior indicado para diretor-presidente com mandato de seis anos, Coronel Arthur Pereira Sabbat e Joacil Basilio indicados como diretores com mandatos de cinco e quatro anos, respectivamente, Nairane Farias Rabelo e Miriam Wimmer indicadas como diretoras com mandatos de três e dois anos, respectivamente.

6 - Qual a formação exigida para atuar como DPO?

Resposta: A LGPD não estabelece uma formação obrigatória e específica para o profissional que pretende atuar como DPO. Isso vale tanto para a GDPR, quanto para a LGPD. Ainda assim, é aconselhável que esse profissional tenha um bom conhecimento das leis e práticas do setor, tendo em vista a necessidade de habilidades híbridas, tanto com conhecimento em legislação quanto conhecimentos técnicos voltados a cibersegurança e governança de dados.

O desafio, portanto, é escolher alguém que possua competência técnica para desempenhar todas essas funções de maneira específica para a organização, conhecendo seus processos internos, objetivos estratégicos e as regulamentações próprias do setor. O cargo pode ser ocupado por pessoas físicas, jurídicas, internos ou terceirizados.

7 - Quando a empresa ao³ terá o sistema no formato da LGPD (contratos de trabalhos) e qual segurança que vamos ter no sistema?

Resposta: Cada empresa possui características próprias e cada contrato deve ser sempre analisado e validado pela área jurídica da empresa, não sendo possível fornecer modelos de contratos de trabalho sem conhecer tais características. Por esse motivo, cada empresa deverá estabelecer as regras e previsões contratuais que atenderão seu negócio.

Sobre a segurança dos sistemas da **ao³**, maiores informações podem ser acessadas em nossa **Política de Privacidade:** **https://info.ao3tech.com/politica-de-privacidade.** Abaixo, destacamos um trecho do documento.

Segurança, conservação e armazenamento de informações:

Mantemos a segurança de suas informações aplicando medidas técnicas de proteção contra o tratamento não autorizado ou ilícito, bem como contra a perda, destruição ou danificação acidental. Faremos todo o possível para proteger suas informações pessoais, apesar de não podermos garantir a segurança das informações que forem transmitidas para nosso website, aplicações ou serviços, ou para outros websites, aplicações e serviços, através da Internet ou de uma ligação idêntica. No caso de lhe termos dado (ou de você ter escolhido) uma senha para acessar determinadas áreas de nossos websites, aplicações ou serviços, recomendamos guardar a senha em lugar seguro e nunca partilhar com ninguém.

*Se tiver razões para acreditar que a segurança de sua conta foi comprometida, contate-nos através do endereço **privacidade@ao3tech.com**. Reforçamos que os dados são armazenados de acordo com as normas de prescrição do direito brasileiro.*

8 - Para admissões, usamos um formulário com as informações pessoais do novo funcionário, porém elas vêm por escrito e algumas empresas ainda encaminham cópias de documentos. Esses dados e documentos impressos devem ser descartados ou podemos arquivar?

Resposta: É necessário analisar todas as informações que são coletadas nesse formulário e ver se ele está adequado ao Princípio da Necessidade.

O que o Princípio da Necessidade estipula é que a coleta de dados deve se dar de maneira restritiva, prezando pelo tratamento estritamente necessários ao atendimento da finalidade pretendida, dispensada a coleta excessiva. Se a finalidade dos dados coletados no formulário foi atingida e não existe nenhuma lei ou norma que justifique o arquivamento do documento, a recomendação é de que, após a utilização seja realizada a eliminação segura dos dados que atingiram sua finalidade no processo de admissão.

A LGPD trouxe consigo uma lista de dez princípios e diretrizes que servem como norteadores para todas as normatizações específicas previstas em seu texto legal. São eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

9 - No contrato de trabalho é necessário colocarmos uma cláusula, referente a LGPD?

Resposta: Sim. Entendemos que todos os contratos de trabalho devem ser revistos e analisados com o apoio da área jurídica da empresa, que precisará atualizar os documentos segundo as normas previstas pela LGPD.

10 - Como os pequenos escritórios de contabilidade poderão se adequar à LGPD sendo que não há folga financeira? O alto custo poderá inviabilizar a continuidade da atividade dos pequenos. Pergunto: como e de que forma a ao³ poderá ajudar na adequação à legislação (LGPD)?

Resposta: A LGPD é para todas as empresas que de alguma maneira realizam o tratamento de dados pessoais com finalidades comerciais. A LGPD estabelece uma série de medidas que devem ser adotadas pelos agentes de tratamento, as quais incluem a identificação das bases legais que justifiquem as atividades de tratamento de dados, a adoção de processos e políticas internas que assegurem o cumprimento das normas de proteção de dados pessoais e o estabelecimento de um canal de contato com os titulares de dados pessoais. Um projeto de adequação à LGPD não precisa ter alto valor de investimento, o processo pode ser iniciado com ações mais simples e entregas pequenas.

Essa será uma jornada constante e o processo de conformidade à LGPD pode acontecer aos poucos, um passo de cada vez seguindo a realidade de cada empresa.

A ao3 tem promovido eventos, webinars e workshops como este para apoiar os escritórios no início de sua jornada de adequação. Também oferecemos, junto à IOB Educação, cursos e treinamentos para ajudá-los com conhecimento especializado sobre a LGPD. Esses recursos podem ser acessados em: **https://www.iobeducacao.com/portal-lgpd-iob**

11 - Nos escritórios de contabilidade, o que precisaremos ter para proteger os dados de nossos clientes? Seria um programa, um contrato?

Reposta: A LGPD estabelece uma série de medidas que devem ser adotadas pelos agentes de tratamento, as quais incluem a identificação das bases legais que justifiquem as atividades de tratamento de dados, a adoção de processos e políticas internas que assegurem o cumprimento das normas de proteção de dados pessoais e o estabelecimento de um canal de contato com os titulares de dados pessoais.

O que toda empresa que quer se adequar à LGPD precisa nesse momento é implementar um Programa de Governança e Privacidade e para isso poderá se orientar pelo artigo 50º, que descreve as regras e boas práticas de governança.

O projeto de adequação é composto por vários processos e etapas internas, que poderão ser melhor implantados com a ajuda de um Programa de Governança e Privacidade. O PGP deve reunir os requisitos de privacidade e segurança e tem o intuito de orientar como os dados pessoais serão manuseados em seu ciclo de vida como um todo.

12 - Quem tem um escritório de contabilidade precisará fazer um termo de consentimento de tratamento de dados para clientes PJ ao firmar contrato de prestação de serviço?

Reposta: Isso vai depender do tipo de tratamento que será realizado. Se há um contrato de prestação de serviços, há uma base legal para determinados tratamento de dados. Contudo, se o tratamento dos dados exceder a finalidade, sim, terá que ser obtido o consentimento pontual para determinadas atividades, conforme previsto no art. 7º, inciso I da LGPD.

13 - Os dados coletados pela contabilidade não tem prazo definido, por quanto tempo ficam armazenados no nosso sistema?

Reposta: Nesse contexto, tudo dependerá se há leis e regulamentos específicos que exigem tempo mínimo para a guarda de determinados dados.

Sugerimos o desenvolvimento de uma Política de Retenção de Dados que deixe claro a todos da organização, bem como aos seus parceiros, os prazos de retenção institucionalmente estabelecidos em conformidade com leis e regulamentos vigentes.

Devemos lembrar que todos os tratamentos de dados pessoais devem ser limitados no tempo. Portanto, após a implementação da Política de Retenção de Dados em sua empresa, todo novo tratamento realizado por qualquer colaborador ou parceiro deverá seguir as determinações descritas no documento. Para além dos tópicos da política, é interessante criar uma tabela anexa com o cronograma para apagamento dos dados – contendo a categoria dos dados pessoais, o período de retenção (obrigatório) e o responsável.

Outro ponto importante é que independentemente do término do tratamento e sua exclusão – seja pela exclusão ao fim do contrato, por prazo legal ou a pedido do titular dos dados – quando cabível, a organização deverá manter um log das atividades referentes à eliminação de dados pessoais para poder comprovar que cumpriu com seu respectivo dever, caso venha a ser questionada.

Sugestão de tópicos para a **Política de Retenção**:

- Finalidade e escopo;
- Público-alvo;
- Documentos de referência;
- Regras de retenção;
- Princípios gerais de retenção;
- Cronograma geral de retenção;
- Responsabilidade pela salvaguarda dos dados durante o período de retenção;
- Violações de dados e conformidade;
- Cronograma geral de destruição;
- Casos omissos;
- Validade;
- Anexo (cronograma);

14- Ao determinar um DPO, preciso formaliza-lo de alguma forma?

Reposta: Sim. O DPO é exigido por lei e embora a LGPD nada diga a respeito de um instrumento de nomeação, recomenda-se ao menos criar um termo específico sobre a função, para delimitar com clareza as atribuições e responsabilidades do cargo.

Se for um DPO externo, é melhor fazer um contrato de prestação de serviços. Se o DPO for um colaborador antigo, submetido ao regime CLT, pode-se fazer um aditivo contratual para constar essa função. A organização precisa criar 3 documentos a respeito do DPO:

1. Documento com a descrição das funções do DPO (semelhante a uma política interna):

- Finalidade do DPO;
- Posição na organização;
- Responsabilidades;
- Autoridade do DPO;
- Casos omissos;
- Validade.

2. Documento de sua nomeação: Texto corrido indicando o fundamento legal para a nomeação, sua vinculação às funções a serem exercidas, a quem se reporta (se foro caso), e uma referência aos Termos de Nomeação.

3. Documento com os Termos da Nomeação:

- Contexto e finalidades do DPO na organização;
- A descrição do mandato do DPO deve:
  - Ser acessível a todos
  - Conter detalhes de contato
  - Garantir a independência do DPO
  - Descrever as obrigações de segredo e/ou confidencialidade
  - Determinar o papel da organização em relação ao DPO
  - Estabelecer a responsabilidade do DPO

15 - As empresas podem contratar um DPO pessoa física?

Reposta: Existem três modalidades de DPO. A escolha por uma delas deverá ser feita segundo as características de cada empresa. A saber:

Colaborador da organização: Pode ser um colaborador antigo, a quem se atribui nova função ou alguém contratado (pessoa física) especificamente para ser o encarregado de dados.

Pessoa natural externa (consultor): O encarregado externo é um prestador de serviço, que pode ser também chamado de “DPO as a service” (DPOaaS). Trata-se de um contrato de consultoria mensal, geralmente assumido por um profissional liberal. Esse profissional muitas vezes é um advogado ou analista de TI, mas também pode ser de outras áreas. Há lugares em que os contadores exercem essa função. A lei deixa isso totalmente livre.

Pessoa jurídica: É uma empresa que presta serviços como encarregado de dados, geralmente contando com uma equipe multidisciplinar. Tudo o que se disse sobre o DPOaaS pessoa natural, aplica-se ao encarregado do tipo pessoa jurídica, com a diferença de que geralmente as empresas que prestam esse serviço possuem uma equipe multidisciplinar.

16 - E para aquelas empresas que não tem website, como nomear um DPO?

Reposta: O encarregado de proteção de dados, também conhecido como DPO, é a pessoa responsável por auxiliar as empresas que fazem tratamento de dados pessoais a cumprirem as obrigações legais referentes à privacidade. Assim, o DPO deve atuar como uma ponte de comunicação entre as empresas, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

A LGPD estipula que a identidade e as informações de contato do DPO devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site de quem controla os dados pessoais, conforme descrito no artigo 41, § 1º. Se a empresa ainda não possui um site, é recomendado criar um. Isso também ajudaria a consolidar uma área de relacionamento com o titular, inclusive para atender os direitos previstos no artigo 17 e 18, através da qual o titular pode enviar suas solicitações. É importante que a empresa crie um canal de comunicação com seus titulares e com a Autoridade Nacional de Proteção de Dados – órgão do governo responsável por fiscalizar

a aplicação das regras estabelecidas pela LGPD.

Isto significa que qualquer empresa que colete dados pessoais deverá indicar publicamente, de preferência no site, quem é o encarregado (DPO) da empresa e as informações de contato desse profissional.

17 - Como é a ação da ANPD?

Reposta: A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil. A missão institucional da ANPD é assegurar a mais ampla e correta observância da LGPD no Brasil e, assim, garantir a devida proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

O art. 55-J da LGPD estabelece as principais competências da ANPD, dentre as quais se destacam as seguintes:

- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e de Privacidade;

- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

- Promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança para toda a população;

- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;

• Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

• Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à lei;

• Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, suas competências e casos omissos;

• Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;

• Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

(fonte: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd)

18 - Ferramentas como Google Drive, Telegram e Whatsapp; são indicadas para realizar trocas de dados?

Reposta: Uma ferramenta adequada é aquela que consegue fornecer segurança e proteção dos dados no momento da troca e fornece privacidade aos usuários. É preciso, por exemplo, garantir o controle de acesso a informações pessoais. Infelizmente, determinadas ferramentas, podem expor os dados de clientes.

Nesse sentido, indicamos que sejam sempre compartilhadas informações sigilosas apenas em meios seguros. Apesar de parecer óbvio, muitas vezes nós nos comunicamos por meios que não são seguros, e acabamos compartilhando informações extremamente sensíveis.

Muitos profissionais utilizam canais de comunicação como WhatsApp, Telegram, e-mail e Messenger para se comunicar com seus clientes. Tirar dúvidas e criar relacionamento digital por esses canais é uma ótima prática para aspectos como fidelização, mas é fundamental que nenhum dado sigiloso seja compartilhado através dessas ferramentas.

Informações como dados de cartões, logins e senhas, não devem ser compartilhadas. Se por algum motivo você precisa comunicar essas informações, faça por ligação ou por meio de plataformas seguras, com criptografia e controle de acessos dos usuários.

19 - LGPD tem alguma relação com os tipos de documentos solicitados na admissão de um funcionário?

Reposta: A LGPD tem relação com todo e qualquer tipo de documento que contenha dados pessoais de pessoa natural, identificada ou identificável, conforme estabelecido no art. 5º, incisos I e II.

20 - Posso organizar o Comitê de Privacidade e Proteção de Dados Pessoais por departamentos?

Reposta: A criação de um Comitê de Privacidade e Proteção de Dados Pessoais não é uma obrigação legal, trata-se, sem dúvida, de um instrumento facilitador da promoção de uma cultura de proteção aos dados pessoais dentro da organização, ao mesmo tempo que contribui para a tomada de decisão de forma centralizada, com a minimização, inclusive, de eventuais conflitos de interesse.

A LGPD impõe ao controlador e ao operador a obrigação de manutenção dos registros das operações de tratamento de dados pessoais, de modo que eles devem não só cumprir a lei mas sobretudo demonstrar a adoção de medidas técnicas e organizacionais necessárias para o adequado cumprimento desta.

Desse modo, a constituição de um Comitê de Privacidade e Proteção de Dados Pessoais pode representar um importante passo no cumprimento de tal exigência.

O comitê fornecerá uma visão empresarial sobre a proteção de dados pessoais, e seus integrantes deverão:

- propor políticas, ajudando no gerenciamento de atividades relativas ao tratamento de dados, entre outros.

- ser, preferencialmente, pessoas envolvidas diretamente nos processos/atividades empresariais e/ou que tenham amplo conhecimento dos principais processos de DP e RH, Jurídico, Financeiro, Comercial, Marketing, SAC, etc. Além disso, é preciso que tenham ampla aderência aos valores da empresa.

21 - Nosso escritório capta os dados e os insere nos sistemas da AO3. Quem seriam os responsáveis pela implementação da LGPD, nós ou a ao³?

Reposta: Os dois são responsáveis. O seu escritório que capta os dados é o Controlador responsável a quem compete as decisões sobre os dados captados. A ao³ a depender do tipo de serviço que está sendo prestado, poderá ser enquadrada como Operadora ou Controladora adjunta no tratamento de dados pessoais, pois o sistema recebe e processa determinados dados. Mas o que realmente definirá as responsabilidades de cada um é aquilo que foi estabelecido em contrato e as políticas acordadas entre as partes.

22 - A LGPD impõe termos para uso de dados, certo? É preciso oferecer essa informação com clareza ao titular, explicando como e para que serão utilizados seus dados?

Reposta: Correto. Essas informações podem ser definidas por meio de uma Política de Privacidade. De acordo com a política de privacidade da empresa é que serão estabelecidas e informadas aos titulares todas as informações referentes à proteção dos dados coletados, a finalidade de tratamento e demais especificações previstas em lei.

23 - Trabalho no departamento pessoal de um escritório pequeno. Hoje já não fico mais com cópias de documentos de funcionários, uso o documento original e o devolvo assim que possível. Tem algo mais que possa ser feito?

Reposta: Nesse fluxo de trabalho citado, o importante é mapear o período de posse dos documentos e registrar tanto a coleta, quanto a exclusão (devolução).

Para todas as empresas que coletam dados pessoais, será necessário adequar seus processos, sistemas e contratos segundo a LGPD. É importante que seja identificado, desde o primeiro momento de coleta de informações pessoais, os seguintes aspectos:

- Finalidade de seu uso;
- Quem poderá ter acesso aos dados e por qual motivo;
- Transparência do processo, para que o titular saiba como seus dados estão sendo tratados, garantia dos direitos dos titulares, que basicamente vão desde o conhecimento de todos os dados que a empresa possui, até a possibilidade de solicitação de exclusão, modificação ou revogação do consentimento de uso desses dados.

24 - As empresas ME e MEI também deverão se adequar à LGPD?

Reposta: Conforme previsto no art. 3º da LGPD, sim, todas as pessoas e empresas que coletam informações de pessoas, sejam elas de clientes ou não, precisam se adequar à LGPD. As únicas hipóteses de dispensa de aplicação da LGPD estão previstas no art. 4º da referida lei.

Entenda as siglas mencionadas neste material:

ANPD – Autoridade Nacional de Proteção de Dados;
Art. – artigo a que se refere o dispositivo de Lei;
CLT – Consolidação das Leis do Trabalho;
DP – Departamento Pessoal;
DPO – Data Protection Officer. A sigla em inglês, foi utilizada na GDPR (lei do Reino Unido de Proteção de Dados Pessoais). No Brasil utiliza-se o termo “encarregado”, mas ambos estão corretos;
LGPD – Lei Geral de Proteção de Dados;
ME – Microempresa;
MEI – Microempreendedor Individual;
PGP – Pretty Good Privacy (Privacidade Muito Boa). Mecanismo de criptografia que fornece autenticação e privacidade criptográfica para comunicação de dados;
RH – Recursos Humanos;
SAC – Serviço de Atendimento ao Cliente;

Para finalizar

Nós, da IOB – uma marca ao³ – queremos agradecer por sua presença no evento, além da confiança depositada em nossos conteúdos.

Estamos à disposição para tirar qualquer dúvida que não tenha sido respondida neste material e esperamos ter ajudado em seu processo de adequação à Lei Geral de Proteção de Dados Pessoais.

A gente se vê em um próximo workshop!

Até lá!

Equipe

IOB, uma marca ao³

Conteúdo: Juliane Borsato, coordenadora de privacidade na ao³
Pesquisa e Revisão: Elaine R. Silva, coordenadora jurídica na ao³