# Manual de Conduta Interno à Proteção de Dados

DRS AUDITORES

1. Regras e Procedimentos
2. Entidade responsável pelo tratamento
3. O Encarregado pela Proteção de Dados
4. Princípios
5. Definição de dados pessoais
6. Tratamento de dados pessoais
7. O Consentimento livre e esclarecido
8. Direitos dos titulares dos dados pessoais
9. Coleta e Gestão de dados dos colaboradores
10. Colaboradores em contato com dados pessoais
11. Cuidados no cotidiano
12. Compartilhamento de dados
13. Tempo de armazenamento dos dados
14. Violação de dados pessoais
15. Proteção de dados e medidas de segurança
16. Políticas de Privacidade de Dados
17. Informação e Formação
18. Contato e Dúvidas

## 1. A proteção de dados pessoais

A proteção de dados pessoais é um direito fundamental da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, como consta no artigo 1º da Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados - LGPD.

A proteção definida pela LGPD cujo Código busca dar cumprimento: "*aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados*", desde que:

> I - A operação de tratamento seja realizada no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Esta proteção deve ser garantida não só pelas autoridades internacionais e nacionais, mas também pelas empresas que devem cumprir a lei e garantir a efetividade dos direitos dos titulares dos dados pessoais.

A defesa dos direitos e liberdades dos titulares dos dados exige uma responsabilidade multidisciplinar dentro da empresa, ou seja, não cabe apenas a um setor, mas sim de uma colaboração conjunta de todos os envolvidos.

O tratamento de dados pessoais deve ser realizado de forma lícita e adequada, ao mínimo necessário às atividades da empresa, de forma a garantir a segurança dos dados. Esse tratamento deve ser sempre realizado mediante o consentimento do titular dos dados, salvo em casos de obrigação legal. É nesta medida que cumpre à DRS Auditores a elaboração do presente Código de Conduta no que se refere à Proteção de Dados Pessoais, com vistas a definir as boas práticas e os princípios que devem nortear a atuação de todos os colaboradores na empresa.

A DRS Auditores adota políticas e procedimentos de acordo com os valores que defende e em concordância com os padrões estabelecidos pela LGPD.

Esse documento tem como objetivo divulgar os valores padrões de forma integral dentro da empresa, servindo como um instrumento de base a ser praticado por todos os seus colaboradores.

## 2. Contexto e objetivos

O presente Código busca determinar os princípios éticos e profissionais a serem cumpridos por todos os colaboradores no desempenho de suas atividades profissionais ou quando estiverem representando a DRS Auditores. Além disso, busca comprovar que a empresa dispõe de medidas e políticas que garantem o nível de proteção de dados exigidos pela Lei.

As práticas e diretrizes que serão dispostas neste documento se aplicam a todos os funcionários independente de cargos ou setor de atuação e seu cumprimento é de caráter obrigatório. Em caso de não cumprimento, poderá constituir infração passível de procedimento disciplinar dentro da empresa. Para que este documento seja monitorado e aperfeiçoado constantemente, a DRS Auditores nomeou um encarregado pela Proteção de Dados que deverá atuar nas funções previstas na Lei e garantir o cumprimento deste manual.

## 3. Regras e Procedimentos

Nesse Código, consideram-se colaboradores os que tenham uma relação de trabalho, estágio, prestação de serviços ou outro equiparável com a DRS Auditores. Todos os referenciados são individualmente responsáveis pelo cumprimento das disposições legais e regulamentares previstas nas situações de tratamento de dados pessoais.

Os Diretores Executivos e os gerentes de cada departamento, além de cumprirem com as regras dispostas neste documento, devem desempenhar um papel ativo, implementarem e garantirem medidas e recursos para o bom funcionamento dos procedimentos relativos à Proteção de Dados.

A confidencialidade deve ser obrigatoriamente garantida pelos colaboradores como parte indissociável de suas atividades exercidas, além disso, destaca-se a importância de agir em conformidade com toda formação e instrução recebida, inclusive as dispostas neste manual.

Mediante aprovação da Diretoria Executiva o DPO pode, no seu campo de atuação, determinar a implementação de novas medidas, conforme a necessidade, devendo para este fim dispor de controles e acessos adequados e do apoio de todas as áreas envolvidas. Ao DPO, também deve ser relatado possíveis falhas no âmbito do presente Código.

## 4. Entidade responsável pelo tratamento

Os dados da empresa responsável pelo tratamento dos dados são as seguintes:

Nome: DRS Auditores

Endereço: R. Felicissimo de Azevedo, 53 - São João, Porto Alegre - RS, 90540-110

CNPJ: 05.858.335/0001-69

Telefone: (51) 3343-5556

## 5. O encarregado de proteção de dados

O controlador elegeu um encarregado de proteção de dados chamado de DPO tendo como principal atributo atuar como o agente de comunicação e ser responsável por monitorar, orientar e administrar a cultura de Privacidade de Dados, assim como, zelar pelo cumprimento deste manual dentro da empresa visando a conformidade com a LGPD. Além disso, o DPO será responsável por identificar novos possíveis riscos e atualizar as medidas de segurança a nível de tratamento de dados, bem como, sugerir propostas de melhorias. Não obstante, o DPO pode contar com o auxílio de um Comitê de Proteção de Dados, o qual é facultativo a criação pela empresa.

Na DRS Auditores esse responsável eleito foi o Sócio Evandro Sander Pinto, cujo endereço de e-mail é evandrosander@drsauditores.com.br. Estes dados para contato devem estar divulgados de maneira clara e acessível no site da empresa em um canal específico para comunicações e esclarecimentos.

Ressalta-se que é permitido ao DPO exercer outro cargo/função dentro da empresa, desde que não haja conflitos de interesse. Além disso, a Lei não prevê responsabilização do encarregado por danos, a não ser nos seguintes casos de ressalva, como:

Art.186 (CC) Aquele que, por ação ou omissão voluntária, negligência ou

imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 927 (CC) Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.

## 6. Princípios

Conforme as diretrizes constantes no Art.7 da Lei 13.709/2018, a quem se destina este Código, deve-se ser observado e cumprido os seguintes princípios ao tratar dados pessoais:

1. **Finalidade**: deve ser explícito e informado ao titular, as finalidades do tratamento dos dados;

2. **Adequação:** o tratamento deve ser compatível com aquilo que foi informado ao titular;

3. **Necessidade:** tratamento limitado ao mínimo necessário para o alcance da finalidade inicial;

4. **Livre acesso:** acesso fácil e gratuito, aos titulares, sobre como é a forma que os dados pessoais são tratados pela empresa;

5. **Qualidade dos dados:** garantir os dados exatos, claros e atualizados aos titulares, conforme a necessidade do tratamento;

6. **Transparência:** disponibilizar de forma transparente as informações sobre o tratamento, aos titulares;

7. **Segurança:** estabelecer medidas de segurança, para proteger os dados pessoais de situações acidentais ou ilícitas;

8. **Prevenção:** utilizar medidas que previnam a ocorrência de danos aos titulares;

9. **Não discriminação:** impedir que o tratamento seja realizado para atos discriminatórios ilícitos ou abusivos;

10. **Responsabilização e prestação de contas:** demonstração das medidas adotadas, inclusive da sua eficácia, para o cumprimento das normas e princípios que se referem à proteção de dados pessoais.

## 7. Definição de Dados Pessoais

Consideram-se dados pessoais toda a informação relativa a uma pessoa identificada ou identificável. Por identificável, considera-se uma pessoa natural que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, que pode ser o nome, número de identificação, dados de localização (endereço IP), email ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

Existe ainda uma categoria de dados sensíveis, que são aqueles que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. Estes dados devem ser tratados apenas nas hipóteses estabelecidas pela LGPD e ainda, deve haver um cuidado maior em relação à proteção dos mesmos.

## 8. Tratamento de Dados Pessoais

No que se refere a tratamento de dados pessoais, o Artigo 5º da Lei 13.709/2018 enumera uma série de atividades que são consideradas tratar dados, como: coleta, utilização, acesso, distribuição, processamento, armazenamento, eliminação, modificação, dentre outros.

De acordo com o Artigo 7º as hipóteses permitidas por Lei para ocorrer o tratamento de dados pessoais são:

I - mediante o fornecimento de consentimento pelo titular;

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;

IV - para a realização de estudos por órgão de pesquisa garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos

preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

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);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Em casos de alterações em alguma operação de tratamento de dados realizada na empresa, o DPO e os titulares das devidas alterações deverão ser comunicados de forma a verificar a conformidade com as normas.

Os dados coletados devem ser exclusivamente os necessários às atividades da empresa, com sua devida finalidade e não podem ser utilizados para fins opostos aos que motivou sua coleta e foi exposto aos titulares. Esses dados coletados devem seguir o princípio da qualidade do dado, listados anteriormente.

É condição de legitimidade de tratamento que o titular dos dados esteja devidamente informado da finalidade do tratamento a que estarão sujeitos os seus dados pessoais.

## 9. O consentimento livre e esclarecido

O consentimento é a manifestação livre e inequívoca por parte do titular, informando que concorda com o tratamento de seus dados para uma finalidade específica, não podendo haver vício de consentimento. É uma autorização necessária para algumas finalidades fora da relação contratual quando se trata de clientes e da laboral em se tratando de funcionários. Esse consentimento deve ser demonstrado por escrito ou por qualquer outro meio que comprove a manifestação da vontade do titular.

Para ser válido, deve ter sido fornecido de forma livre e esclarecida, ou seja, todas as informações necessárias foram concedidas ao titular como o fundamento e a finalidade do tratamento, quais dados são coletados, o operador e o controlador, se há compartilhamento de dados e o prazo que esses dados ficarão armazenados, logo em casos de autorizações genéricas, serão consideradas nulas. O titular pode revogar seu consentimento a qualquer momento.

## 10. Direitos dos Titulares de Dados Pessoais

A LGPD estabelece procedimentos que visam proteger e efetivar os direitos dos titulares dos dados, devendo estes serem adotados pela DRS Auditores.

Direitos que são assegurados a todos os titulares de dados:

- confirmação da existência do tratamento de seus dados pela empresa;
- acessar os dados que a empresa possui;
- solicitar a correção e a atualização dos dados;
- anonimização, bloqueio ou eliminação de dados além do necessário ou tratados de forma destoante com o previsto em Lei;
- portabilidade dos dados a outro fornecedor de serviços ou produtos;
- eliminação dos dados, salvo nas hipóteses previstas no Art. 16 da Lei;
- informações das entidades às quais houveram compartilhamento dos dados do titular;
- informações sobre a consequência do não fornecimento do consentimento;
- revogar o consentimento.

Para exercer os seus direitos, utilize os meios de contato disponibilizados no Website da DRS Auditores ou pelo formulário de solicitação disponível no Canal de Privacidade do site.

## 10. Coleta e gestão de dados de colaboradores

É permitido o tratamento dos dados desde que, eles sejam necessários e possuam medidas para proteção. Logo, os dados são tratados não só conforme a legislação em vigor, mas também de acordo com o que está estabelecido nos contratos de trabalho.

Além disso, juntamente com a assinatura do Contrato de Trabalho, a DRS Auditores

deve solicitar ao colaborador o seu consentimento expresso para situações como as que constam a seguir:

- Divulgação de fotos de funcionários em redes sociais, para fins de endomarketing;
- Compartilhamento de dados com empresas terceiras para diferentes necessidades.

Lembre-se que, deve haver um consentimento para cada finalidade, além de medidas de conversação dentro da empresa para fins de prova de legitimidade.

São coletados dados pessoais de colaboradores nas finalidades de procedimentos como o processo de admissão, demissão e cumprimento de obrigações fiscais e trabalhistas.

Neste caso acima, eventualmente, podem ser coletados, inclusive, dados pessoais sensíveis como origem racial e informações médicas e de saúde, devendo estes serem tratados com maior confidencialidade.

O tratamento dos dados pessoais e suas respectivas finalidades deverão estar descritas no contrato de trabalho.

## 11. Colaboradores em contato com dados pessoais

Os colaboradores que realizem qualquer tratamento de dados pessoais como o acesso, coleta, uso, armazenamento, dentre outros, estão obrigados ao sigilo profissional e confidencialidade sobre os mesmos, sendo vedado divulgar ou utilizar esses dados para fins diferentes de suas atividades estabelecidas no contrato. Exceto em casos previstos em Lei, como por exemplo, quando o poder público os exija para execução de políticas públicas.

Sendo assim, é imprescindível uma responsabilidade por parte dos clientes e fornecedores no que se refere à segurança dos dados pessoais.

## 12. Cuidados no cotidiano

Realizar o tratamento de dados pessoais exige um elevado nível de cuidados e para isso é necessária uma atenção por parte dos colaboradores em suas rotinas na empresa.

Em se tratando de armazenamento, sempre que possível, os documentos devem ser preferencialmente guardados em formato digital, com níveis de acesso bem definidos nos sistemas (cada colaborador com seu login e senha) visto que, os documentos impressos são mais passíveis de serem acessados por outros colaboradores. Se for necessário que os

documentos sejam impressos, deve-se tomar cuidado com papéis deixados na impressora, pois podem ser facilmente copiados.

Cada colaborador é responsável pela documentação que está em sua posse, devendo comprometer-se pela guarda dessa informação. Além disso, após a conclusão do prazo de armazenamento e a finalidade tenha sido cumprida, toda a documentação física com dados pessoais deverá ser descartada de forma segura, ou seja, rasurada e rasgada.

Ressalta-se que, alguns cuidados devem ser praticados com os computadores como: não deixar as senhas visíveis, não deixar documentos abertos quando não estiver presente e optar sempre pelo bloqueio de tela numa ausência.

Ainda, destaca-se que a DRS está em processo de readequação do seu ambiente de trabalho, de modo que dificulte que as conversas e troca de informações sejam ouvidas por outros funcionários.

Por fim, sugere-se que os funcionários realizem a troca de suas senhas, e que esta, seja uma palavra passe segura e seja mantida em sigilo.

## 13. Compartilhamento de dados

Em caso de contratação de serviços de empresas terceirizadas que necessitem de acesso a dados de clientes ou colaboradores para prestar serviço à DRS Auditores, deve-se adotar todas as medidas de segurança e protocolos estabelecidos no que corresponde à proteção de dados pessoais e o cumprimento do manual.

Por meio dos entregáveis do Programa de LGPD será possível estabelecer um compromisso maior referente à proteção da confidencialidade e segurança dos dados pessoais da empresa, assim como, prevenir o acesso e utilização indevida, perdas ou destruição não autorizada de dados pessoais.

Além disso, mediante o Manual de Due Diligence (ferramenta elaborada no programa de proteção de dados pessoais com vistas à negociação com terceiros), a DRS Auditores se compromete a contratar empresas que apresentarem níveis suficientes de proteção de dados para assegurar a defesa dos direitos de clientes e colaboradores.

Na hipótese de cumprimento de obrigações como funções de interesse público ou o exercício da autoridade pública, existe a obrigação de fornecimento de determinados dados pessoais, dentro do absolutamente necessário para a finalidade em causa.

## 14. Tempo de armazenamento dos dados

O armazenamento dos dados deve possuir um prazo definido. Quando o dado pessoal não estiver mais sendo utilizado para o fim o qual foi coletado, deverá ser eliminado, caso não haja uma nova finalidade.

Os dados serão mantidos pelos prazos mínimos que constam nas leis, de acordo com o caráter específico.

Sugere-se que, documentos como currículos e processo de seleção, sejam armazenados por no máximo 1 ano e documentos de caráter geral pelo prazo de 5 anos. Por fim, documentos trabalhistas e previdenciários devem ser armazenados conforme orientações do guia "Prazo de guarda de documentos", com seus respectivos amparos legais.

## 15. Violação de dados pessoais

Vale lembrar que o conceito de violação de dados pessoais deve ser de conhecimento de todos os colaboradores. A violação vai além da simples perda de dados pessoais, é caracterizada por uma falha de segurança que pode motivar destruição, perda, alteração, divulgação ou acesso não autorizado. Essa violação tem que provocar efeitos como discriminação, ameaça à reputação, perda financeira, perda de confidencialidade ou qualquer outra desvantagem social ou econômica significativa. Mais do que uma consciência individual, é de responsabilidade de todos, estarem atentos a possíveis violações de dados e comunicar ao DPO da DRS Auditores por meio do endereço de email evandrosander@drsauditores.com.br.

Após analisar o possível fato relatado, se o DPO julgar que houve violação com riscos e consequências, deve comunicar à Autoridade Nacional de Proteção de Dados - ANPD, preenchendo o modelo de notificação de incidentes em um prazo de até 72 horas. Para analisar a situação ocorrida, é necessária uma colaboração conjunta dos departamentos, inclusive um auxílio nas medidas que possam minimizar ou corrigir tal incidente.

## 16. Proteção de dados e medidas de segurança

Os colaboradores devem fazer o uso de dispositivos e ferramentas que lhes são disponibilizados exclusivamente para fins profissionais e de forma diligente zelando pela

manutenção, sendo proibida a troca de periféricos ou a abertura de equipamentos informáticos sem autorização expressa da Direção.

Nota-se que na DRS Auditores alguns acessos são restritos à alta gestão e aos gerentes de alguns departamentos. No entanto, faz-se necessário uma revisão de acordo com os riscos dispostos no Relatório de Impacto à Proteção de Dados Pessoais -RIPD, os quais são relacionados à concessão de acessos definidos aos colaboradores de cada departamento, visto que, em algumas situações, ainda pode se notar acessos indevidos.

Em relação à proteção de dados e medidas de segurança presentes no setor de Tecnologia da Informação - TI evidencia-se na DRS Auditores: dispõe de antivírus AVG pago, se resguardando contra ataques cibernéticos e ransomwares, evitando possíveis vazamentos e roubo de dados; o software utilizado para organização interna e revisão de arquivos é o Caseware, sendo que a empresa pode vir a avaliar uma possível proteção desse software; e, por fim, há possibilidade de acesso remoto aos dispositivos via senha de rede individual.

## 17. Políticas de Privacidade de dados

A DRS Auditores busca estar sempre em cumprimento com as exigências vigentes na Lei, a exemplo têm-se as práticas como o desenvolvimento e atualização contínua da Política de Privacidade de Dados, a qual pode ser encontrada no site da empresa ou ser solicitada diretamente ao DPO.

## 18. Informação e formação

Toda a informação relacionada a este Código e as medidas adotadas para o seu cumprimento serão disponibilizadas a todos os colaboradores da DRS Auditores. O DPO deve promover ações de formação a todos os envolvidos, bem como a divulgação do regulamento de modo que todos os colaboradores fiquem informados.

## 19. Contato e dúvidas

Para dúvidas sobre a aplicação das regras da Lei e das regras listadas no presente Código, os colaboradores podem entrar em contato com o DPO da empresa. Tudo aquilo

que o Código não abranger, deverá ser considerado o que está previsto na Lei 13.709/2018.