CLARIENS EDUCAÇÃO S.A.

Companhia Fechada
CNPJ/ME nº 48.199.560/0001-43
NIRE 35.3.0060203-0

POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

CAPÍTULO I
OBJETIVO E ABRANGÊNCIA

Artigo 1º. Esta Política Geral de Privacidade e Proteção de Dados ("Política") tem como objetivo dar as diretrizes gerais e reforçar que a Clariens Educação S.A., suas controladas e mantidas ("Companhia") está(ão) comprometida(s) com a privacidade e a proteção dos dados pessoais de todas as pessoas que de alguma forma se relacionem com a instituição.

Artigo 2º. Faz parte da nossa missão a construção de uma cultura organizacional voltada para a transparência, privacidade e segurança da informação. Ou seja, a preocupação com esses valores faz parte do nosso dia a dia.

Artigo 3º. Por isso é muito importante que todas as pessoas que utilizam dados pessoais em nome da Companhia, suas controladas e mantidas, sejam elas colaboradores ou parceiros, sigam rigorosamente as orientações desta Política, que estabelece as diretrizes para boas práticas em proteção de dados pessoais.

Artigo 4º. Entende-se por 'Colaborador' todos os funcionários, estagiários e aprendizes vinculados à Companhia, suas controladas e mantidas, independentemente do cargo ou função exercida, enquanto 'Parceiro' são todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais, fornecedores e representantes com quem a Companhia se relacione.

Artigo 5º. A presente Política foi dividida em 12 capítulos: I. Objetivo e Abrangência; II. Definições; III. Base Legal para Tratamento de Dados; IV. Dados dos Titulares; V. Tratamento de Dados Pessoais na Companhia; VI. Privacidade de Dados Pessoais por Concepção e por Padrão; VII. Obrigação de Confidencialidade; VIII. Padrões de Segurança. IX Monitoramento do Programa de Proteção dos Dados Pessoais e Auditoria; X. Atribuições e Responsabilidades; XI. Canais de Comunicação; e XII. Disposições Gerais.

Artigo 6º. Importante mencionar que este documento não substitui as regras estabelecidas nos contratos de trabalho, de prestação de serviços ou outros termos de compromisso relativos à privacidade que o colaborador ou parceiro esteja vinculado.

CAPÍTULO II
DEFINIÇÕES

Artigo 7º. Para a melhor compreensão desta Política, os termos nela mencionados possuem as seguintes definições:

Base legal: São as hipóteses previstas na LGPD que autorizam o tratamento de dados pessoais. O uso de qualquer dado pessoal necessita se enquadrar em uma dessas hipóteses da lei.

Controlador: É quem determina as finalidades e a forma como os dados vão ser tratados. A Companhia é a controladora dos dados pessoais de seus colaboradores, leads e clientes.

Dado pessoal: Toda informação, relacionada à pessoa física, capaz de torná-la identificada ou identificável. Ou seja, dado pessoal pode se referir a um único dado, que seja capaz de identificar alguém, como o CPF, RG ou por exemplo uma foto, ou um conjunto de informações que combinadas, podem levar a identificação de determinada pessoa, como um número de matrícula, endereço, características físicas, entre outros.

Dado pessoal sensível: É um tipo especial de dado pessoal, pois seu uso em determinadas situações pode oferecer mais riscos para as pessoas. São considerados sensíveis os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Dado de criança e adolescente: A LGPD também dá atenção especial aos dados pessoais das crianças e adolescentes. São consideradas crianças as pessoas até 12 anos de idade (incompletos) e adolescentes as pessoas entre 12 e 18 anos de idade.

Dado anonimizado: É o dado que originalmente era pessoal, mas após a aplicação de algumas técnicas, passou a não possibilitar a identificação do titular. Por exemplo, quando temos uma tabela constando apenas o telefone e o Estado de determinado grupo de alunos, e trocamos os dígitos do telefone por uma sequência idêntica de carácter ((xx)xxxxx-xxxx) de modo que não seja mais possível a identificação da pessoa. Se o dado for anonimizado, a LGPD não se aplica. Para tornar um dado anonimizado, o procedimento aplicável deve ser irreversível e suficiente para que não seja possível a identificação do titular, por isso o procedimento precisa ser orientado pelo Comitê de Privacidade e pelo time de Tecnologia da Informação.

Encarregado: É a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela implementação, fiscalização e cumprimento da LGPD.

Finalidade: É o propósito que a Companhia deseja alcançar com a utilização de determinado dado. Podemos ter várias finalidades para um mesmo dado, contudo, todas elas precisam estar previamente avaliadas. Por exemplo, usamos o nome do aluno para a emissão de boletos, para emissão de documentos, tais como diploma e histórico escolar, entre outros. Cada um desses usos tem uma finalidade específica.

Incidente de Segurança da Informação: Qualquer ocorrência relacionada a violação na segurança de dados, esteja ele em meio físico ou digital, como acesso não autorizado, perda, vazamento, destruição ilícita entre outros.

LGPD: Lei Geral de Proteção de Dados Pessoais. É a lei que estabelece as regras para a utilização e tratamento dos dados pessoais no Brasil.

Operador: Pessoa física ou jurídica que realiza o tratamento de dados em nome do Controlador. Na Companhia trabalhamos com diversos operadores, tais como empresas que fornecem serviços de tecnologia, agências de marketing, entre outras. Os operadores devem utilizar os dados pessoais conforme as orientações recebidas do controlador.

Relatório de Impacto: É a documentação elaborada pelo controlador que contém o levantamento dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares, bem como, as medidas para proteção, mitigação ou eliminação dos riscos identificados.

Responsável legal: É a pessoa física que recebe por lei, decisão judicial ou procuração, a atribuição de representar outra pessoa. É importante entender este conceito, pois na LGPD, alguns direitos e atos só podem ser exercidos pelo titular ou seu representante legal.

Segurança da Informação: É um conjunto de regras, metodologias e práticas utilizadas para preservar a informação da empresa, seja ela em meio físico ou digital. São exemplos de medidas de Segurança da Informação, utilização de antivírus, senhas fortes, controle de acesso aos arquivos físicos, entre outros.

Tratamento de dados pessoais: Qualquer atividade realizada com os dados pessoais. A lei traz como exemplos a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração. Ou seja, é tudo aquilo que fazemos com o dado pessoal.

Titular: É o dono do dado pessoal que está sendo tratado. No caso da Companhia, suas controladas e mantidas são exemplos de titulares os nossos parceiros, alunos, colaboradores, leads (possíveis clientes), visitantes e usuários de serviços das clínicas, serviços de saúde e dos núcleos de práticas jurídicas.

Artigo 8º. A Lei Geral de Proteção de Dados Pessoais, estabelece alguns princípios que devem ser observados quando do tratamento de dados pessoais. Esses princípios funcionam como diretrizes que devem orientar nossa conduta toda vez que pensamos em utilizar os dados pessoais.

Artigo 9º. Desta forma, ainda que não haja uma regra específica sobre determinado assunto, os princípios podem nos auxiliar a tomar a decisão que melhor garanta a proteção dos dados que estamos tratando. Vamos conhecê-los?

Princípio da finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com

essas finalidades (exemplo: Não usar os dados de alguém que demonstrou interesse em um determinado produto ou serviço para ofertar outro produto não associado àquele);

Princípio da adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (exemplo: Não usar o e-mail do aluno para enviar comunicações não relacionadas à área de educação);

Princípio da necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (exemplo: Para fazer um questionário de satisfação precisamos pedir nome, e-mail e telefone ou basta o número da matrícula do aluno? basta a matrícula);

Princípio do livre acesso: Garantia aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (exemplo: Não pode haver cobrança aos titulares para informá-los sobre seus próprios dados);

Princípio da qualidade dos dados: Garantia aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (exemplo: Permitir a retificação de nome, CPF, e-mails etc., que eventualmente estejam incorretos ou desatualizados em nossos cadastros);

Princípio da transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (exemplo: Informar ao titular sobre a coleta de cookies quando ele navegar em nosso site, de forma clara e visível);

Princípio da segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (exemplo: Não compartilhar senhas com terceiros);

Princípio da prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (exemplo: Investimento em treinamentos dos colaboradores);

Princípio da não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (exemplo: Não realizar o tratamento de determinado dado pessoal nos currículos, como orientação religiosa, para impedir o acesso do titular às fases seguintes do processo seletivo)

Princípio da responsabilização e prestação de contas: Demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (exemplo: Registrar as auditorias realizadas, documentar as orientações feitas aos fornecedores através de contratos e acordos de processamento de dados).

CAPÍTULO III

BASES LEGAIS PARA TRATAMENTO

Artigo 10º. As bases legais são as hipóteses previstas na LGPD que autorizam o tratamento de dados pessoais.

Artigo 11. Agora, vamos falar daquelas que se aplicam às instituições da Clariens e sua utilização dentro da Companhia.

1. **Cumprimento de obrigação legal ou regulatória:** Quando precisamos utilizar determinado dado para cumprir ou atender alguma legislação a qual estamos submetidos, como por exemplo, quando compartilhamos os dados pessoais dos alunos com o Ministério da Educação para a realização do censo escolar.

2. **Execução do contrato ou procedimentos preliminares:** Quando precisamos utilizar determinado dado para cumprir um contrato que tem como parte o próprio titular e a Companhia. Por exemplo, quando utilizamos o nome do aluno para emissão do boleto, usamos a base legal de execução de contrato, pois sem o pagamento da mensalidade, não podemos oferecer as aulas que ele contratou.

3. **Exercício regular de direitos:** Quando precisamos utilizar o dado para nos defender em processos judiciais ou administrativos. Por exemplo, quando precisamos apresentar os documentos acadêmicos de determinado aluno em ações movidas por este.

4. **Proteção à vida ou incolumidade física:** Quando utilizamos o dado pessoal para proteger a vida ou a integridade física de alguém, como por exemplo a medição de temperatura nas portarias, para identificar potenciais infectados por Covid-19.

5. **Tutela da saúde:** Quando precisamos utilizar os dados para proteger a saúde de um titular, desde que este tratamento seja feito pelo profissional de saúde. Por exemplo, quando solicitamos os dados dos pacientes que são atendidos em nossas clínicas de saúde.

6. **Legítimo Interesse:** Quando precisamos utilizar os dados para atender a interesses legítimos da Companhia ou de terceiros. A LGPD não define exatamente as situações que se configuram como legítimo interesse, por isso sua aplicação deve acontecer a partir de situações concretas, levando-se em conta a finalidade, necessidade e proporcionalidade. Utilizamos o legítimo interesse, por exemplo, quando fazemos pesquisa de satisfação com nossos alunos.

7. **Consentimento:** Quando utilizamos determinado dado mediante manifestação de vontade expressa do titular. Por exemplo, quando solicitamos do titular o consentimento para envio de propagandas e publicidade para seu e-mail ou telefone. Essa manifestação precisa ser livre, informada e inequívoca. Isso significa que o titular não foi obrigado a concordar com os termos do documento que solicita o consentimento, que o consentimento não foi colhido de forma automática, que o titular leu e compreendeu todas as informações, que devem ser passadas de forma clara e simples, e que ele não está assinando o documento com dúvidas.

Artigo 12. Quando se tratar de dados sensíveis, algumas dessas bases legais não poderão ser utilizadas para respaldar a utilização dos dados, tais como execução do contrato ou legítimo interesse. Neste caso, precisamos ser ainda mais cautelosos.

Artigo 13. Nos casos da utilização de dados de crianças e adolescentes, também precisamos de cuidados adicionais. A Lei Geral de Proteção de Dados Pessoais reserva um capítulo especial para a proteção dos dados pessoais de crianças e adolescentes e estabelece que o tratamento de dados nestes casos precisa ser realizado no melhor interesse do menor.

Artigo 14. Com relação às crianças, pessoas de até 12 (doze) anos de idade incompletos, obriga ainda que seja dado o consentimento livre, inequívoco, específico e em destaque, fornecido pela mãe, pai ou responsável legal. Ou seja, nestes casos, independente de lei ou contrato, precisamos em regra, do consentimento para tratar os dados da criança.

CAPÍTULO IV
DADOS DOS TITULARES

Artigo 15. Os titulares possuem diversos direitos relacionados aos seus dados pessoais e a Companhia está empenhada em observar e garantir o exercício desses direitos.

Artigo 16. Os principais direitos dos titulares são:

1. Confirmar se estamos realizando o tratamento dos seus dados;
2. Ter acesso às informações sobre a forma e a duração de tratamento dos dados pessoais e com quem a Companhia compartilha os seus dados
3. Solicitar a atualização ou correção dos seus dados;
4. Solicitar a anonimização, bloqueio ou eliminação dos dados pessoais tratados;
5. Portabilidade dos dados a outro fornecedor de serviço ou produto;
6. Possibilidade de não fornecer o consentimento e quando fornecer, solicitar a revogação, devendo ser informado das consequências da negativa e/ou revogação;

Artigo 17. Naturalmente, o exercício de alguns desses direitos podem inviabilizar a continuidade da prestação de serviços, por exemplo, não temos como atender um paciente em uma de nossas clínicas se precisarmos eliminar seus dados de saúde. Além disso, tendo em vista que temos obrigações legais e regulatórias a cumprir, nem sempre poderemos atender todas essas solicitações. Por isso, as solicitações devem ser avaliadas caso a caso pelo comitê de privacidade e as pessoas por ele designadas.

Artigo 18. Desta forma, caso um titular de dados entre em contato para exercer esses direitos, deve ser direcionado para os seguintes canais:

Inserir link de direcionamento ao One Trust
ou então por e-mail:
privacidadededados@clariens.com.br

Artigo 19. Se o titular não tiver acesso à canais digitais, deverá fazer a sua solicitação em uma de nossas unidades, com auxílio de nossos atendentes, conforme fluxo de atendimento ao titular, estabelecido pelo Comitê de Privacidade.

Artigo 20. Importante ressaltar que nossos parceiros devem comunicar imediatamente ao Encarregado, se receberem qualquer solicitação de um titular, com relação aos dados pessoais tratados em decorrência do contrato com a Companhia e não devem responder a esta solicitação, salvo se houver disposição expressa no contrato de prestação de serviço, convênio ou parceria comercial em sentido contrário. A notificação deverá ser enviada para: privacidadededados@clariens.com.br

CAPÍTULO V
TRATAMENTO DE DADOS PESSOAIS NA COMPANHIA

Artigo 21. A Companhia realiza o tratamento de diversos Dados Pessoais, para a execução de atividades regulares de ensino e pesquisa, e outras de apoio àquelas.

Artigo 22. Mas é importante que todos os princípios e os direitos dos titulares aqui mencionados, sejam observados neste tratamento. Por isso, ao realizar qualquer atividade de tratamento, seja a coleta de uma informação, armazenamento de algum dado, ou mesmo a confecção de uma planilha de controle, sempre verifique se todas as diretrizes de proteção de dados estão sendo cumpridas.

Tratamento dos Dados Pessoais

Artigo 23. A Companhia realiza o tratamento de diversos dados pessoais para que o negócio aconteça. A relação de dados tratados inclui: dados pessoais comuns, como os de identificação, contato, da própria navegação (endereço de IP e cookies), dados pessoais sensíveis, como os de saúde, etnia e raça, biométricos e outros dados eventualmente necessários para execução da finalidade das atividades prestadas, de acordo com a relação existente entre a Companhia e o titular dos dados, e com obrigações legais que a Companhia tenha que cumprir.

Artigo 24. Ao fazer o tratamento de dados pessoais, devemos nos ater aos dados estritamente necessários para o desenvolvimento da nossa atividade e para o cumprimento das leis e regulamentos aos quais estamos obrigados.

Artigo 25. Além disso, dados pessoais só poderão ser coletados através de acessos a bases públicas ou privadas (ou seja, de forma indireta) se avaliadas pelo Comitê de Privacidade.

Artigo 26. O tratamento realizado por parceiros em nome da Companhia, deve estar documentado por meio de contratos de prestação de serviços, de parceria ou convênios. Isto vale também para dados fornecidos por terceiros à Companhia.

Finalidade e uso dos Dados Pessoais

Artigo 27. A utilização dos Dados Pessoais está vinculada à expectativa que o titular dos dados possuía no momento da coleta das informações. Ou seja, o uso dos dados está limitado à finalidade informada ao titular.

Artigo 28. A finalidade do uso dos dados é informada ao Titular do Dados Pessoais através de contratos, termos, comunicados e principalmente através do aviso de privacidade e proteção de dados pessoais.

Artigo 29. Por isso, havendo necessidade de alteração da finalidade, esta precisa ser informada ao titular antecipadamente. O Comitê de Privacidade também deve ser envolvido previamente, para orientar quanto a legalidade do tratamento do dado para a nova finalidade e para atualização dos registros de tratamento.

Artigo 30. E isso vale para os nossos parceiros também. Eles não poderão utilizar os dados pessoais tratados em decorrência da atividade exercida para a Companhia, para finalidade diferente da acordada através dos instrumentos contratuais.

Artigo 31. Quando os Dados Pessoais forem utilizados para análises preditivas ou decisões automatizadas, é necessário que se registre toda a documentação da lógica utilizada para construir o modelo, passando pelos dados utilizados, as análises empregadas para embasar a escolha desses dados e a forma como esses dados foram inseridos no modelo. Além disso, os modelos precisam ter acompanhamento constante para verificar se por algum motivo começou a enviesar e discriminar as pessoas no seu processo de predição/clusterização.

Artigo 32. Isto porque é um direito do titular ter informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Além disso, a autoridade de proteção de dados poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Artigo 32. Por fim, em casos de aquisição de outras empresas e expansão do negócio, é imprescindível a análise do Comitê de Privacidade desde o momento das negociações, pois a aquisição de um negócio que não atua em conformidade com a legislação de privacidade e proteção de dados, pode trazer prejuízos futuramente para a Companhia.

Registro de Atividades de Tratamento de Dados Pessoais

Artigo 34. A Companhia é obrigada por lei, a registrar todas as atividades de tratamento que realiza e manter esse registro atualizado.

Artigo 35. Por isso, todos aqueles que tratam Dados Pessoais em nome da Companhia, devem colaborar para a manutenção deste registro informando eventuais inconsistências, alterações ou criação de atividades de tratamento e o encerramento dessas atividades ao Encarregado. O parceiro também deve informar à Companhia qualquer alteração que implique mudanças importantes na gestão interna dos dados pessoais objeto dos contratos e convênios firmados, nos termos estabelecidos nesses documentos.

Artigo 36. O Encarregado é responsável por garantir a atualização e revisão periódica completa deste registro juntamente com cada departamento.

Artigo 37. O registro do tratamento, deve conter no mínimo, as seguintes informações: descrição da atividade, quais dados são tratados, local de armazenamento, com quem os dados são compartilhados, finalidade do tratamento, tempo de retenção do dado, base legal para tratamento, idade dos titulares dos dados e volume aproximado de registros.

Compartilhamento de Dados Pessoais

Artigo 38. No dia a dia muitos Dados Pessoais precisam ser compartilhados com colegas de trabalho e parceiros, para a realização das atividades da Companhia. Mas neste compartilhamento, algumas regras precisam ser observadas.

Artigo 39. Dentro da Companhia, os Dados Pessoais devem ser compartilhados apenas com as pessoas cuja função exija que elas tenham acesso a eles. O compartilhamento deve ser feito apenas pelos meios corporativos disponibilizados e homologados pelo time de Tecnologia da Informação – TI na política de Segurança da Informação, tais como e-mail e drive corporativo.

Artigo 40. Por exemplo, dados referentes aos dependentes, como os constantes nos formulários de plano de saúde, só podem ser compartilhados dentro da Companhia com pessoas que sejam responsáveis pelo tratamento dessas informações, como colaboradores do departamento de Recursos Humanos, não podendo ser compartilhados com colaborador da área acadêmica que não precise ter acesso a esses dados para o cumprimento de suas funções.

Artigo 41. Já no compartilhamento de Dados Pessoais com os parceiros externos, as informações compartilhadas devem ser aquelas estritamente necessárias para a realização da atividade contratada, por e-mails e drives corporativos ou através de sistemas homologados pela TI. [No caso de compartilhamento de arquivos, estes devem estar preferencialmente protegidos por senhas, que não devem ser enviadas juntamente com o arquivo em questão].

Artigo 42. Os dados só devem ser compartilhados em meio físico, quando for inevitável. Neste caso, o documento deve ser entregue diretamente para quem deve recebê-lo, por pessoa autorizada ou contrato para o transporte de documentos e de preferência com assinatura em livro protocolo.

Artigo 43. Os parceiros que tratam Dados Pessoais em nome da Companhia, não devem nomear ou divulgar quaisquer dados recebidos para qualquer operador subcontratado, a menos que previamente exigido ou autorizado pela Companhia por meio dos instrumentos contratuais cabíveis. E neste caso, deverão cobrar, fiscalizar e garantir que estes subcontratados tenham níveis padrão de segurança e cumpram toda a legislação aplicável neste tratamento.

Transferência internacional dos Dados Pessoais

Artigo 44. Determinados serviços podem demandar a transferência dos Dados Pessoais tratados pela Companhia para outros países, como por exemplo, para empresas de tecnologia que prestam serviço de armazenamento em nuvem. Nesses casos, os dados devem ser tratados de acordo com a Lei Geral de Proteção de Dados Pessoais e demais legislações aplicáveis. Adotamos cláusulas padronizadas nos

contratos com fornecedores e prestadores de serviço para garantir o mesmo nível de privacidade, segurança e confiabilidade no tratamento dos dados.

Artigo 45. O parceiro não pode transferir ou autorizar a transferência de Dados Pessoais para fora do Brasil sem o consentimento prévio por escrito da Companhia.

Armazenamento dos Dados Pessoais

Artigo 46. Nos casos dos dados digitais, estes devem ficar armazenados em local seguro, protegido por criptografia e com restrição de acesso por senha.

Artigo 47. O local de armazenamento dentro da Companhia deve ser necessariamente homologado pela TI conforme política de Segurança da Informação. Não estão autorizados o armazenamento de dados pessoais [em área de trabalho ou HD do computador do usuário], e-mails ou contas pessoais, ou ainda em pendrive, CDs, ou outros dispositivos remotos, salvo se expressamente autorizado pelo Comitê de Privacidade.

Artigo 48. No caso de Dados Pessoais em meio físico, estes devem ficar em local protegido por chave e com controle e registro de acesso. Os documentos contendo dados pessoais não devem ser utilizados como rascunho ou ficar em local de fácil acesso, tais como mesas ou bancadas de escritórios, impressoras, entre outros.

Artigo 49. Quando armazenados provisoriamente na casa de um colaborador, os documentos devem ser mantidos em locais seguros, preferencialmente em locais fechados com chave e longe do alcance de outras pessoas não autorizadas. Documentos que não estão em uso deverão ser imediatamente devolvidos para o arquivo da Companhia.

Artigo 50. Eventuais cópias de arquivos contendo Dados Pessoais somente devem ser feitas se necessárias para o cumprimento da atividade ou de legislação a qual estamos sujeitos, devendo ser mantidas com o mesmo grau de proteção que os arquivos originais. O controle dessas cópias, sejam digitais ou físicas, devem ser documentadas, para possibilitar a eliminação assim que terminado o objetivo do tratamento, de acordo com a política de descarte da Instituição.

Eliminação dos Dados Pessoais

Artigo 51. O Dado Pessoal também possui um ciclo de vida. Desta forma, decorrida a finalidade para qual o dado foi coletado e tratado, e não havendo mais necessidade de mantê-lo para cumprir alguma obrigação legal ou regulatória, os mesmos devem ser eliminados.

Artigo 52. A Lei Geral de Proteção de Dados Pessoais regulamentou o direito à eliminação de dados, com objetivo de proporcionar ao titular, maior controle das suas informações pessoais.

Artigo 53. A eliminação de dados pessoais também deve ser feita de forma segura. Por isso uma Política de Retenção e Descarte de Dados Pessoais será divulgada, para esclarecer o período e a forma de descarte dos dados pessoais tratados pela Companhia. Enquanto ela não for divulgada, o Comitê de Privacidade irá fazer as orientações para cada departamento.

Artigo 54. Além disso, nossos parceiros também devem devolver à Companhia e posteriormente excluir ou obter a eliminação de forma segura, todas as cópias e Dados Pessoais tratados em razão do nosso contrato ou parceria, findada a finalidade de tratamento, sendo papel do gestor do contrato este monitoramento.

Artigo 55. Os prazos para a devolução e eliminação dos Dados Pessoais, constarão na Política de Retenção e Descarte [e o Comitê de Privacidade deverá ser comunicado toda vez que este processo ocorrer]. [Se tratando de dados disponíveis em sistema, o departamento de Tecnologia da Informação também deve ser comunicado].

Tratamento de Dados Pessoais Sensíveis

Artigo 56. Dados Pessoais sensíveis serão tratados apenas quando for imprescindível para alcançar a finalidade proposta, geralmente para cumprir obrigações legais e regulatórias, como nos casos dos Dados Pessoais Sensíveis tratados pelo departamento de recursos humanos e acadêmico, para concessão de benefícios e defesa em processos como os tratados pelo departamento jurídico e núcleos de práticas jurídicas, ou para a tutela da saúde, como nas clínicas de saúde.

Artigo 57. Dados Pessoais Sensíveis devem receber prioridade na Política de Segurança da Informação. O departamento de Tecnologia da Informação deve estar empenhado em garantir a máxima segurança desses dados em nossos sistemas e servidores.

Artigo 58. Contudo, também podemos adotar algumas práticas para proteger esses dados no nosso dia a dia:

1. Restrinja ao máximo o acesso ao Dado Pessoal Sensível, inclusive dentro do departamento;
2. Mantenha os arquivos salvos no [google drive] corporativo protegidos por senha;
3. Priorize o compartilhamento de Dados Pessoais Sensíveis pelo [google drive] corporativo, mas se for necessário compartilhar por e-mail, confirmar se os destinatários estão corretos;
4. Tente manter os Dados Sensíveis em tabelas separadas dos outros dados de identificação, de forma que para se chegar neste dado, seja necessário o acesso da outra tabela, preferencialmente salvos em outras pastas. Caso os dados precisem ficar na mesma planilha, mantenha as colunas ou abas com esses dados ocultas enquanto não estiver utilizando os dados;
5. Quando possível, colete o Dado Pessoal Sensível apenas do titular que precise ter determinado direito resguardado. Por exemplo, não precisamos coletar a orientação religiosa de todos os alunos para garantirmos o direito à guarda religiosa, basta coletar o dado do aluno que queria exercer este direito;
6. Não utilize ferramentas gratuitas para trabalhar com dados pessoais, sobretudo os sensíveis, salvo se expressamente autorizados pelo departamento de Tecnologia da Informação e pelo Comitê de Privacidade.

Tratamento de dados de crianças e adolescentes

Artigo 59. Na Companhia, também utilizamos dados de crianças e adolescentes. Mas, estes dados só devem ser solicitados de forma excepcional, quando necessário para o cumprimento do contrato, cumprir nossas obrigações legais ou garantir algum direito do menor.

Artigo 60. Na Companhia, não será permitida em nenhuma hipótese o tratamento de dados de menores de 12 anos para envio de publicidade e propagandas.

Artigo 61. Caso por alguma razão a Companhia deva receber dados de qualquer menor de 12 (doze) anos incompletos, devemos colher o consentimento, livre, inequívoco, específico e em destaque, fornecido pela mãe, pai ou responsável legal, salvo em situações excepcionais, para contactar os pais ou responsáveis ou para a proteção do menor.

Artigo 62. O Comitê de Privacidade deve ser acionado para a confecção destes documentos e avaliação da atividade de tratamento.

Artigo 63. Além disso, devemos realizar todos os esforços razoáveis para verificar se este foi dado pelo responsável pela criança.

CAPÍTULO VI

PRIVACIDADE DE DADOS PESSOAIS POR CONCEPÇÃO E POR PADRÃO

Artigo 64. A Companhia deve assegurar a proteção dos dados pessoais, mas essa proteção deve ser feita, pela Companhia, de forma proativa e preventiva e não reativa.

Artigo 65. Por isso, adotamos o modelo de *privacy by design,* ou privacidade desde a concepção. Desta forma, a Companhia entende que desde a criação do serviço, projeto, sistema, produto ou processo, a privacidade e proteção de dados precisa ser observada, acompanhando todo o ciclo de vida da atividade desenvolvida.

Artigo 66. Segundo a própria LGPD, as medidas de segurança, técnicas e administrativas para proteção de Dados Pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço.

Artigo 67. Além disso, devemos empregar o *privacy by default* ou privacidade por padrão. Isso significa que nos nossos produtos ou serviços, as medidas de privacidade estruturadas na fase de concepção, devem ser aplicadas como regra.

Artigo 68. Por isso, todo novo processo ou atividade a ser desenvolvida em qualquer setor da Companhia, deve ser comunicada ao Comitê de Privacidade ou ao Encarregado de Proteção de Dados, desde o início do planejamento, para que sejam realizadas as avaliações necessárias com vistas a desenvolver um processo adequado à legislação e baseados nestas metodologias.

CAPÍTULO VII

OBRIGAÇÃO DE CONFIDENCIALIDADE

Artigo 69. Para garantir a segurança e privacidade dos Dados Pessoais, também devemos adotar medidas que resguardem o sigilo e a confidencialidade das informações.

Artigo 70. Um dado confidencial, é aquele que deve ser resguardado contra a revelação pública não autorizada, seja de forma escrita ou falada. Serão considerados como confidenciais, todos os Dados Pessoais tratados pela Companhia, sobretudo os Dados Pessoais Sensíveis e de menores de idade.

Artigo 71. Por isso, os colaboradores e parceiros da Companhia que tiverem acesso a esses dados, devem mantê-los no mais estrito sigilo, obrigando-se a não divulgar, revelar ou mostrar a terceiros, salvo quando autorizado expressamente pela Companhia ou quando for inerente ao desenvolvimento da atividade, de acordo com o contrato de trabalho ou prestação de serviços. Também é proibido usar tais Dados Pessoais em seu próprio benefício comercial ou pessoal, direta ou indiretamente.

Artigo 72. Algumas medidas para preservar a confidencialidade dos dados:

1. Não imprimir ou fazer cópia de arquivos com informações confidenciais, salvo nos casos em que for necessário para desenvolvimento das atividades de interesse da Companhia.
2. Quando a impressão ou cópia for necessária, elas devem ser descartadas com segurança logo após atingir sua finalidade e devem seguir as metodologias de segurança desta Política, da Política de Retenção e Descarte de Dados Pessoais e da Política de Segurança da Informação;
3. Não circular em ambientes externos com cópias desses dados, salvo quando estritamente necessário;
4. Não tecer comentários ou discutir sobre dados confidenciais em ambientes públicos.

Artigo 73. O colaborador ou parceiro que estiver na posse e guarda de arquivos confidenciais será o responsável por sua conservação (preservação contra danos, perda entre outros) integridade (mantê-los confiáveis e consistentes em todo seu ciclo de existência) e manutenção de sua confidencialidade (não permitindo que as informações e dados sejam disponibilizados ou divulgados a quem não tenha autorização para tanto).

Artigo 74. Salvo nos casos em que o compartilhamento de informações for inerente à atividade desenvolvida, tais como envio de informações à Receita Federal, Ministério do Trabalho e Ministério da Educação, feitas pela contabilidade, RH e Diretoria acadêmica por exemplo, as informações confidenciais ou sigilosas só poderão ser enviadas às autoridades públicas pelo colaborador, após orientação do Departamento Jurídico e de Compliance em conjunto com o Comitê de Privacidade e/ou Encarregado de Proteção de Dados.

Artigo 75. O colaborador deverá respeitar o sigilo e a confidencialidade das informações que os parceiros compartilharem conosco. Essas informações devem ser tratadas com o mesmo cuidado que as informações sigilosas da própria Companhia.

Artigo 76. Ainda que as informações se tornem de domínio público, perdendo o seu caráter confidencial, devemos continuar com as medidas de proteção dos Dados Pessoais e seguir os princípios estabelecidos pela lei, tais como guarda segura, uso para a finalidade estabelecida, retenção pelo prazo necessário, entre outras.

Artigo 77. Havendo dúvida sobre o caráter confidencial e sigiloso da informação, ou sobre a possibilidade de divulgação, consulte o seu gestor, o Departamento Jurídico e de Compliance, Comitê de Privacidade, e/ou Encarregado de Proteção de Dados. O dever e obrigação de sigilo e confidencialidade, continuará vigente mesmo após o término da relação contratual.

CAPÍTULO VIII

PADRÕES DE SEGURANÇA

Artigo 78. A LGPD estabelece que a empresa deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais dos mais diversos tipos de incidentes.

Artigo 79. Para tanto, além do programa de proteção de dados conduzido pelo Comitê de Privacidade, o departamento de Tecnologia da Informação desenvolveu uma Política de Segurança da Informação com as medidas necessárias, relativas às boas práticas de segurança da informação.

Artigo 80. Como referência, a Companhia adotou nesta Política de Segurança da Informação, as medidas previstas nas normas e frameworks da ISO 27001. Um framework de segurança é uma estrutura de processos que tem o objetivo de gerenciar e reduzir riscos de segurança da informação, ajudando a Companhia a proteger os dados em seus ambientes físicos e digitais.

Artigo 81. Contudo, para que a Política de Segurança da informação seja efetiva, todos devem estar comprometidos com as diretrizes que ela estabelece.

Incidentes com Dados Pessoais

Artigo 82. Se houver indicativo de um incidente envolvendo os dados pessoais tratados em nome da Companhia, o colaborador ou parceiro deverá comunicar imediatamente aos **Acionadores do Time de Resposta a Incidentes**, conforme especificado no Plano de Resposta a Incidentes de Segurança e à Privacidade e Proteção de Dados, com todas as informações requeridas e através dos e-mails: privacidadededados@clariens.com.br

Artigo 83. A condução do incidente será realizada de acordo com o Plano de Respostas a Incidentes de Segurança e à Privacidade e Proteção de Dados. Os departamentos e parceiros envolvidos, devem cooperar com a Companhia e tomar as medidas para auxiliar na investigação, mitigação e correção de cada violação de dados pessoais.

CAPÍTULO IX

MONITORAMENTO DO PROGRAMA DE PPROTEÇÃO DE DADOS PESSOAIS E AUDITORIA

Artigo 84. A Companhia fiscalizará as contas corporativas disponibilizadas pela empresa, tais como e-mails, contas de mensagens instantâneas e de teleconferência, além de registros de acesso à Internet, Intranet, ligações e mensagens de texto, informações e arquivos recebidos ou armazenados nos dispositivos físicos, eletrônicos ou digitais, e sistemas de da Companhia.

Artigo 85. A Companhia também utiliza recursos da tecnologia Endpoint, que tem como objetivo garantir que servidores e dispositivos conectados à nossa rede estejam protegidos de ameaças cibernéticas. Para isso, o sistema gerencia permissões de instalação de programas, bem como acessos à aplicativos, páginas de Internet, drives, entre outros.

Artigo 86. O Comitê de Privacidade deverá realizar monitoramento anual para avaliar o nível de conformidade da Companhia em relação a legislação de privacidade, bem como avaliar os processos

que precisam ser melhorados, através de auditorias internas e auditoria independentes, sempre que necessário.

Artigo 87. Algumas medidas que devem ser adotadas são:

1. Aplicação de questionários para avaliação da maturidade da organização;
2. Avaliação do histórico de solicitação dos titulares, relatório de incidentes e denúncias sobre violação às normas;
3. Avaliação do relatório de acessos das contas corporativas e do sistema Endpoint;
4. Auditoria dos fornecedores e parceiros;
5. Revisão dos mapeamentos de tratamento de dados pessoais realizados pelas áreas;

Artigo 88. Além disso, o departamento de Tecnologia da Informação, juntamente com o Marketing e Comitê de Privacidade, devem conduzir anualmente testes de engenharia social, *pentestes* e testes de *phishing* dentro da Instituição**.**

Artigo 89. O teste de engenharia social simula uma manipulação do usuário para que ele revele informações confidenciais ou execute determinadas atividades que ponham em risco a segurança da informação da empresa. Ou seja, seu foco é testar possíveis falhas humanas. Como por exemplo, se passar por um aluno nos canais de atendimento para conseguir informações sigilosas sobre ele.

Artigo 90. O *pentestes* ou teste de intrusão, tem como objetivo detectar eventuais fragilidades de um sistema ou estrutura de segurança digital, para validar as diretrizes utilizadas e monitorar nosso tempo de resposta, caso a intrusão aconteça. Ou seja, a pessoa designada para esta atividade irá simular um ataque às nossas redes e sistemas em busca de vulnerabilidades.

Artigo 91. Já o teste de *phishing* verifica se conseguimos distinguir um conteúdo falso de um verdadeiro, como por exemplo, detectar se conseguimos reconhecer que determinado e-mail é fraudulento e está simulando um fornecedor conhecido, te direcionando para uma página com o intuito de roubar seus dados ou se o e-mail é legítimo.

Artigo 92. Além disso, os parceiros devem disponibilizar ao Comitê de Privacidade, quando solicitado, todas as informações necessárias para demonstrar a conformidade do programa de proteção de dados da instituição, em relação aos dados pessoais que tratar em nome da Companhia.

Infrações

Artigo 93. O descumprimento desta Política pode acarretar a aplicação de medidas disciplinares ou demissão por justa causa para os colaboradores envolvidos, conforme Política de Medidas Disciplinares, aplicação de sanções e rescisão de contrato para os prestadores de serviço, bem como o ajuizamento de ações judiciais cíveis ou criminais, quando aplicável.

CAPÍTULO X
ATRIBUIÇÕES E RESPONSABILIDADES

Artigo 94. A responsabilidade pelo tratamento dos Dados Pessoais de forma adequada dentro da Companhia é comum a todos os colaboradores e parceiros do grupo (terceiros), sendo fundamental a participação de todos para que a Companhia esteja sempre em conformidade com a lei, oferecendo segurança aos titulares dos dados utilizados.

Artigo 95. Neste cenário, alguns órgãos ou departamentos são os responsáveis por estabelecer as diretrizes relacionadas à privacidade e proteção de dados e acompanhar o efetivo cumprimento destas, dentro do ambiente corporativo. Mas lembre-se que independente do setor, cada um desempenha um papel importante no programa institucional de privacidade e proteção de dados!

Artigo 96. Atribuições e responsabilidades do Conselho de Administração:

- Avaliar e aprovar todas as políticas relacionadas ao programa de privacidade, incluindo esta Política e suas futuras alterações;
- Avaliar e aprovar o orçamento para a implementação das medidas de adequação necessária, conforme proposta da Diretoria/Comitê de Privacidade.

Artigo 97. Atribuições e responsabilidades do Comitê de Auditoria, Risco, Governança e Compliance:

- Avaliar e todas as políticas relacionadas ao programa de privacidade, incluindo esta Política e suas futuras alterações e recomendar sua aprovação e/ou eventuais modificações ao Conselho de Administração;
- Avaliar e recomendar ao Conselho de Administração a aprovação do orçamento para a implementação das medidas de adequação necessária, conforme proposta da Diretoria/Comitê de Privacidade;

Artigo 97. Atribuições e responsabilidades da Diretoria:

- Deliberar sobre a estrutura do programa de governança em privacidade e proteção de dados;
- Apoiar o Encarregado de Proteção de Dados em suas atribuições;
- Participar de reuniões periódicas como Comitê de Privacidade e para alinhar as estratégias relacionadas à privacidade e proteção de dados pessoais;

Artigo 98. Atribuições e responsabilidades do Comitê de Privacidade:

- Elaborar e revisar os documentos relativos ao Programa de Privacidade e Proteção de Dados, propondo à Diretoria e ao Conselho de Administração para aprovação;
- Reportar ao Comitê de Auditoria, Risco Governança e Compliance e ao Conselho de Administração todos os eventos relevantes sobre o Programa de Privacidade e Proteção de Dados, tais como riscos e ameaças, incidentes e oportunidades de melhoria;
- Elaborar o orçamento com todos os recursos necessários para a manutenção do programa de privacidade, e submeter à aprovação da Diretoria/ Conselho de Administração;

- Se empenhar para que que a Companhia esteja em conformidade com as legislações que versem sobre privacidade e proteção de dados pessoais;
- Acompanhar o cumprimento pelos colaboradores e terceiros, das políticas e procedimentos internos que versem sobre privacidade e proteção de dados;
- Participar de reuniões periódicas com a Diretoria para alinhar as estratégias relacionadas à privacidade e proteção de dados pessoais;
- Implementar os meios necessários para a preservação dos direitos dos titulares de dados e responder às solicitações dos mesmos, de acordo com a legislação aplicável;
- Cooperar e se relacionar com a Autoridade Nacional de Proteção de Dados Pessoais;
- Estruturar e coordenar a execução de Análise de Impacto de Privacidade de Dados (PIA), Relatório de Impacto de Proteção de Dados (RIPD), testes de proporcionalidade quando o tratamento for baseado no legítimo interesse e formalização de incidentes de Dados Pessoais;
- Orientar gestores, colabores e terceiros quanto a aplicação das leis e diretrizes internas nos projetos de cada área, que envolvam tratamento ou utilização de dados pessoais;
- Desenvolver o programa de conscientização sobre privacidade e proteção de dados na Companhia, elaborando materiais de apoio, treinamentos e avaliações de maturidade;
- Elaborar e realizar acordos internacionais de transferência de dados;
- Acompanhar e auxiliar as áreas na implementação dos planos de ação para correção de falhas que ameacem a segurança e proteção de dados;
- Garantir a manutenção das evidências de execução e implementação das iniciativas de privacidade, mantendo ainda o registro de todas as atividades realizadas pelo Comitê de Privacidade;
- Revisar e manter atualizado o mapeamento de Dados Pessoais, junto aos departamentos, sempre que ocorrer uma mudança substancial no tratamento ou uso de dados pessoais, ou pelo menos, uma vez por ano.
- Gerenciar situações de crise que envolvam dados pessoais tratados pela Companhia, reunindo as informações necessárias sobre o evento, monitorando a repercussão, elaborando o plano de ação para mitigar o impacto e construindo o posicionamento da instituição perante o público interno, externo e reporte às autoridades interessadas.
- Gerenciar os possíveis riscos e ameaças relacionados aos dados pessoais que possam afetar a Companhia, identificando, avaliando, quantificando, qualificando, definindo plano de ação e monitorando cada risco ou ameaça em conjunto com o Comitê de Privacidade e Proteção de Dados**.**

Artigo 99. Atribuições e responsabilidades do Marketing

- Revisar os documentos elaborados pelo Comitê de Privacidade quando necessário;
- Apoiar a elaboração e divulgação de treinamentos sobre privacidade e proteção de dados;
- Publicar avisos de privacidade em websites e programas externos;
- Monitorar a utilização de cookies nos websites institucionais;
- Garantir que os dados pessoais, imagem e voz dos nossos alunos e colaboradores, ou de terceiros, sejam utilizados devidamente nas campanhas realizadas pelas instituições;
- Garantir a coleta e revogação do consentimento dos titulares, juntamente como o Comitê de Privacidade, dentro das suas atividades de tratamento, quando aplicável;
- Disseminar a cultura de privacidade e proteção de Dados Pessoais através de campanhas e e-mails marketing.

Artigo 100. Atribuições e responsabilidades do departamento de Tecnologia da Informação:

- Revisar e manter atualizada a Política de Segurança da Informação e anexos, garantindo a aplicação das normas estabelecidas nos referidos documentos;
- Elaborar o plano de ação para a implementação das normas de segurança da informação, orientando as respectivas áreas e executar aquilo que diz respeito ao setor de tecnologia da informação;
- Implementar medidas técnicas e organizacionais apropriadas, de acordo com as melhores práticas de segurança da informação, para garantir um nível de segurança adequado e proporcional ao risco gerado, em particular, a partir de uma violação de dados pessoais;
- Avaliar os sistemas e ferramentas de tecnologia, informando ao comitê de privacidade as fragilidades do ponto de vista de proteção e segurança dos dados pessoais e as medidas necessárias para a correção destes gaps;
- Indicar do Departamento Jurídico e de Compliance, as cláusulas necessárias para adequação dos contratos e convênios do ponto de vista de Segurança da Informação;
- Auxiliar o Comitê de Privacidade no mapeamento de parceiros que fornecem soluções de tecnologia;
- Acompanhar e realizar a devolução e eliminação de dados pessoais pelos parceiros, conforme prazo e forma acordados em contrato;
- Identificar e analisar as vulnerabilidades dos servidores e sistemas e informar ao Comitê de Privacidade aquelas que possam expor ou tornar vulneráveis dados pessoais;
- Realizar testes, treinamentos e tomar as medidas necessárias para eliminar ou mitigar riscos de violação de dados pessoais;
- Avaliar os incidentes envolvendo dados pessoais, reportando ao Comitê de Privacidade todas as informações relacionadas ao evento que sejam disponíveis, em especial, a quantidade e descrição dos dados envolvidos, os titulares dos dados afetados pelo evento, as evidências técnicas e as medidas adotadas para correção da falha identificada.

Artigo 101. Atribuições e responsabilidades do Departamento de Recursos Humanos

- Contribuir com a coleta de evidências que indiquem a aplicação das regras internas de privacidade e proteção de Dados Pessoais;
- Colaborar para que os contratos de trabalho e de prestação de serviço contenham cláusulas de privacidade e confidencialidade adequadas à legislação e regulamentação aplicáveis;
- Contribuir para que os consentimentos dos colaboradores, quando necessário, sejam devidamente coletados e administrados;
- Apoiar na divulgação de treinamentos sobre privacidade e proteção de dados;
- Prestar as informações necessárias ao Encarregado de Proteção de Dados, para o exercício dos direitos de titular colaborador ou ex-colaborador
- Aplicação de medidas disciplinares e sanções, ou ajuizamento de ação, quando provado o descumprimento desta Política
- Difundir a cultura de privacidade e proteção de Dados Pessoais na contratação de novos colaboradores e terceiros.

Artigo 102. Atribuições e responsabilidades de área específica de Contratos

- Colaborar para que os contratos ou convênios que contemplem o tratamento de Dados Pessoais contenham cláusulas de privacidade adequadas, informando ao Comitê de Privacidade sobre a necessidade de revisão destes documentos;
- Auxiliar na renegociação de contratos com fornecedores e clientes que realizam o tratamento de Dados Pessoais;
- Informar ao Comitê de Privacidade o distrato de contratos com parceiros, para análise de necessidade de devolução e eliminação de dados;
- Manter os contratos e acordos de processamento de dados, armazenados devidamente.

Artigo 103. Atribuições e responsabilidades do Departamento Jurídico e de Compliance

- Colaborar para que os contratos ou convênios que contemplem o tratamento de Dados Pessoais contenham cláusulas de privacidade adequadas, informando ao Comitê de Privacidade sobre a necessidade de revisão destes documentos;
- Prestar apoio jurídico para que as medidas adotadas pelo Comitê de Privacidade não entrem em conflito com outras legislações ou regulamentações aplicáveis ao negócio da Companhia;
- Apoiar na aplicação de medidas disciplinares e sanções, ou ajuizamento de ação, quando provado o descumprimento desta Política;
- Prestar apoio jurídico na ocorrência de incidentes envolvendo Dados Pessoais;
- Apoiar na interação com a Autoridade Nacional de Proteção de Dados Pessoais e outros órgãos fiscalizadores.

Artigo 104. Atribuições e responsabilidades dos Gestores

- Participar das reuniões com o Comitê de Privacidade, sempre que convocados;
- Transmitir aos outros Colaboradores, as ações necessárias para a conformidade de cada departamento ao programa de privacidade elaborado pelo Comitê de Privacidade;
- Apoiar no acompanhamento e na implementação dos planos de ação para correção de falhas das iniciativas de privacidade;
- Contribuir com a fiscalização, auditoria e elaboração dos Indicadores de desempenho e avaliações de maturidade, relacionados à proteção de dados e privacidade, auxiliando na correção de *gaps* remanescentes ou novos que forem identificados.
- Disseminar a cultura de Privacidade e Proteção de Dados Pessoais
- Garantir o uso adequado de Dados Pessoais nas atividades desempenhadas pela sua área, seja pelos colaboradores ou terceiros;
- Informar ao Comitê de Privacidade os requisitos da legislação e regulamentação aplicáveis no respectivo setor, para a conciliação destes com as medidas adotadas no Programa de Governança e Privacidade;
- Consultar o Comitê de Privacidade quando da contratação de parceiros que irão tratar dados pessoais;
- Informar previamente ao Comitê de Privacidade as novas atividades de tratamento ou uso de dados pessoais, bem como qualquer mudança nas atividades já mapeadas;
- Revisar e manter atualizado o mapeamento de Dados Pessoais, junto ao Comitê de Privacidade, sempre que ocorrer uma mudança substancial no tratamento ou uso de dados pessoais, ou pelo menos, uma vez por ano;

- Orientar as áreas de atendimento quanto ao procedimento para solicitação dos direitos dos titulares;
- Assegurar que a coleta de dados com uso de consentimento seja devidamente documentada e cumpra os requisitos da legislação, gerenciando e respeitando as opções do titular caso a caso.

Artigo 105. Atribuições e responsabilidades de todos os Colaboradores e Parceiros da Companhia

- Disseminar a cultura de Privacidade e Proteção de Dados Pessoais;
- Responsabilizar-se pelo uso adequado de dados pessoais em suas atividades;
- Observar e aplicar a legislação e políticas da Companhia sobre privacidade e proteção de dados pessoais, bem como as cláusulas sobre o tema constantes nos convênios, termos, contratos de trabalho, de parceria e prestação de serviço;
- Comunicar ao Comitê de Privacidade, qualquer incidente com dados pessoais ou segurança de dados que tenha conhecimento, bem como as falhas de processos ou procedimentos que possam implicar em riscos de privacidade;
- Comunicar ao Comitê de Privacidade caso tenha conhecimento de potencial conduta que viole as diretrizes dessa Política ou outra norma de proteção de dados;
- Participar dos treinamentos sobre Privacidade e Proteção de Dados Pessoais, quando convocados.

CAPÍTULO XI
CANAIS DE COMUNICAÇÃO

Artigo 106. Ficou com dúvida sobre esta política? Você pode entrar em contato conosco pelo e-mail privacidadededados@clariens.com.br.

CAPÍTULO XII
DISPOSIÇÕES GERAIS

Artigo 107. Qualquer ato contrário ao disposto nesta Política deverá ser reportado à área de LGPD por meio do formulário web disponível no website da Companhia ou através do Canal de Denúncia, para adoção das medidas cabíveis.

Artigo 108. O Colaborador que descumprir quaisquer das determinações previstas nesta Política estará sujeito às sanções previstas no Código de Ética e Conduta e no Política de Medidas Disciplinares, incluindo a rescisão contratual.

Artigo 109. A Companhia se reserva no direito de alterar esta Política. Sempre que isso ocorrer, informaremos a você para renovarmos o nosso compromisso com Privacidade e Proteção de Dados.

Artigo 110. Esta Política será revisada a cada 2 (dois) anos, podendo ser alterada, sempre que necessário ou pertinente, conforme governança da Companhia.

Artigo 111. Os casos omissos e dúvidas de interpretação relativos a essa Política serão tratados por meio de reuniões com o Comitê de Privacidade ou o Comitê de Auditoria, Risco, Governança e Compliance.

Artigo 112. No caso de conflito entre: a) as disposições dessa Política e do Estatuto, prevalecerá o disposto no Estatuto; b) as disposições dessa Política e de acordos de acionistas arquivados na sede da Companhia, prevalecerá o disposto no respectivo acordo de acionistas; e c) em caso de conflito entre as disposições dessa Política e da legislação e regulamentação vigentes, prevalecerá o disposto na legislação e regulamentação vigentes.

Artigo 113. Caso qualquer disposição dessa Política venha a ser considerada inválida, ilegal ou ineficaz, essa disposição será limitada na medida do possível para que a validade, legalidade e eficácia das disposições remanescentes dessa Política não sejam afetadas ou prejudicadas.