MANUAL DE PROTEÇÃO DE DADOS PESSOAIS

PARA GESTORES E GESTORAS PÚBLICAS EDUCACIONAIS

CIEB
CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA

SOBRE O CIEB

O **Centro de Inovação para a Educação Brasileira (CIEB)** é uma organização sem fins lucrativos, cuja missão é promover a cultura de inovação na educação pública, estimulando um ecossistema gerador de soluções para que cada estudante alcance seu pleno potencial de aprendizagem.

Atua integrando múltiplos atores e diferentes ideias em torno de uma causa comum: inovar para impulsionar a qualidade, a equidade e a contemporaneidade da educação pública brasileira.

FICHA CATALOGRÁFICA

Dados Internacionais de Catalogação na Publicação (CIP)
Lumos Assessoria Editorial
Bibliotecária: Priscila Pena Machado CRB-7/6971

M294 Manual de proteção de dados pessoais para gestores e gestoras públicas educacionais [recurso eletrônico] / organização Centro de Inovação para a Educação Brasileira. –– São Paulo : CIEB, 2020.
Dados eletrônicos (pdf).
Inclui bibliografia.
ISBN 978-65-5854-046-5

1. Proteção de dados. 2. Direito à privacidade - Brasil. 3. Escolas - Documentos escolares - Lei e legislação - Brasil. 4. Lei Geral de Proteção de Dados (LGPD). I. Centro de Inovação para a Educação Brasileira (CIEB). II. Título.

CDD 371.272

COMO CITAR ESSE DOCUMENTO
CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA. Manual de Proteção de Dados para Gestores e Gestoras Públicas Educacionais. São Paulo: CIEB, 2020. E-book.

COOPERAÇÃO COM UNESCO
Esta publicação tem a cooperação da UNESCO no âmbito da parceria com o Centro de Inovação para a Educação Brasileira (CIEB) o qual tem o objetivo de apoiar a gestão digital das redes de educação pública no Brasil. As indicações de nomes e a apresentação do material ao longo deste livro não implicam a manifestação de qualquer opinião por parte da UNESCO a respeito da condição jurídica de qualquer país, território, cidade, região ou de suas autoridades, tampouco da delimitação de suas fronteiras ou limites. As ideias e opiniões expressas nesta publicação são as dos autores e não refletem obrigatoriamente as da UNESCO nem comprometem a Organização.

SUMÁRIO

APRESENTAÇÃO

CIEB

O tema da proteção de dados pessoais está na agenda do dia na sociedade, com reflexos também na educação. O aumento no uso de tecnologias educacionais que utilizam dados pessoais nos últimos anos (reforçado pelo contexto atual de pandemia de Covid-19) e a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) reforçam a necessidade de secretarias de educação e redes de ensino se adequarem à lei e garantirem que dados pessoais de estudantes e demais pessoas sejam protegidos.

Além disso, no período pós-pandemia, a adoção de uma educação híbrida, que integre momentos presenciais e remotos, se destacará com um dos meios mais eficazes para ampliar a jornada de aprendizagem dos(as) estudantes – o que demandará atenção especial aos dados pessoais de estudantes, responsáveis legais e docentes ao utilizarem de forma cada vez mais frequente os recursos educacionais digitais.

Neste sentido, o CIEB se adianta a essa necessidade e publica este "Manual de Proteção de Dados Pessoais para Gestores e Gestoras Públicas Educacionais" em parceria com Ronaldo Lemos e sua equipe de advogados e advogadas especialistas em direito e tecnologia e apoio da Fundação Lemann e Imaginable Futures no âmbito do Projeto de Seleção e Aquisição de Tecnologias Educacionais.

O Manual é extenso e completo, pois buscamos traduzir os principais conceitos, princípios da lei e hipóteses da LGPD à realidade das redes de ensino público brasileiras. Com exemplos, linguagem acessível, pontos de atenção, minutas de documentos e orientações sobre todas as etapas do ciclo de vida de dados pessoais na educação pública, esperamos que o Manual seja um documento de apoio e consulta para gestores e gestoras educacionais e auxilie as redes de ensino a coletar, usar e proteger os dados pessoais de forma adequada e segura.

Boa leitura!

Lúcia Dellagnelo, Ed. D
Diretora-Presidente do CIEB

UNESCO

A informação e o conhecimento têm impactado significativamente a vida das pessoas e transformado as sociedades ao redor do mundo, especialmente com o avanço das tecnologias da informação e comunicação (TIC). Apesar de seus desafios, as TIC também representam uma oportunidade para a construção de um mundo mais igualitário, com educação de qualidade, inclusão, paz e desenvolvimento sustentável.

Com o objetivo de contribuir para o alcance desses importantes ideais, a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), cujo mandato abrange o tema da comunicação e informação, tem buscado promover sociedades do conhecimento universais, nas quais as pessoas sejam capazes não apenas de buscar informações, mas também de transformá-las em conhecimento.

No campo da educação, a UNESCO promove o acesso aos conteúdos e às tecnologias por meio da conscientização, da capacitação e do apoio à formulação de políticas e soluções inovadoras, como os Recursos Educacionais Abertos (REA) e a Alfabetização Midiática e Informacional (AMI). Os REA são materiais para ensinar, aprender e pesquisar, que estão em domínio público ou são publicados com uma licença de propriedade intelectual. Eles podem fornecer a estudantes e educadores de todo o mundo um acesso sem precedentes ao conhecimento e à informação. Por outro lado, a AMI busca desenvolver habilidades para que os indivíduos saibam diferenciar conteúdos e se tornem cidadãos mais críticos e ativos, principalmente ao utilizarem as TIC.

Uma importante iniciativa lançada pela UNESCO, em 2013, foi o Currículo de Alfabetização Midiática e Informacional para Formação de Professores. O currículo apresenta a AMI de maneira holística e coloca os professores como os principais agentes de mudança, capazes de alcançar e capacitar milhões de estudantes. Apesar disso, a UNESCO acredita que temas como a ética no uso da internet e a privacidade ainda precisam de atenção.

Resultados iniciais de um estudo produzido pela Aliança Global para Parcerias em Alfabetização Midiática e Informacional, que contou com apoio da UNESCO, indicam que a privacidade é pouco abordada pelos programas de AMI e que falta entendimento entre os educadores sobre os assuntos relacionados à privacidade e como eles se aplicam às competências reais.

A mudança para o ensino a distância, em resposta ao fechamento de escolas devido à pandemia da Covid-19, impulsionou ainda mais as discussões sobre a privacidade e a segurança dos dados de estudantes e professores. Nesse novo contexto educacional, surgem preocupações relativas ao modo como os dados podem ser utilizados para fins comerciais, ou se estudantes e professores estão sendo expostos a anúncios direcionados. Mais do que nunca, é preciso reforçar a necessidade de ambientes saudáveis de informação, mídia e tecnologia.

Com a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil passou a fazer parte do seleto grupo de países que contam com uma legislação específica para a proteção de dados e da privacidade dos seus cidadãos. A legislação brasileira em vigor se fundamenta em diversos valores, como o respeito à privacidade, à liberdade de expressão e aos direitos humanos de liberdade e dignidade das pessoas.

Nesse mesmo sentido, a UNESCO saúda o Centro de Inovação para a Educação Brasileira (CIEB) pela iniciativa de produzir este "Manual de proteção de dados pessoais para gestores e gestoras públicas educacionais", destinado às redes públicas de educação do Brasil. A publicação, que promove a discussão sobre o direito à privacidade entre os gestores da informação das secretarias de Educação de estados e municípios brasileiros, é mais um esforço para ampliar o acesso universal ao conhecimento e à informação no Brasil, com base em valores fundamentais para seus cidadãos.

Além disso, diante de um novo contexto que impacta profundamente todos os aspectos da vida de populações no mundo inteiro, o presente manual se torna um recurso ainda mais relevante para a comunidade educacional pública brasileira, que tem a importante tarefa de garantir a continuidade da educação e da aprendizagem, com segurança e responsabilidade.

Associando-se a essa iniciativa, a UNESCO reforça, assim, o seu compromisso de promover sociedades do conhecimento, nas quais as pessoas possam usufruir plenamente de seus direitos de acesso à informação e desenvolver as habilidades necessárias para se tornarem cada vez mais críticas, participativas e comprometidas com um futuro seguro, justo e resiliente para todos.

Marlova Jovchelovitch Noleto
Diretora e representante da UNESCO no Brasil

FUNDAÇÃO LEMANN E IMAGINABLE FUTURES

Nos dias de hoje, cada interação que fazemos no meio digital deixa uma migalha, um pedaço de informação sobre nossas ações, preferências, características pessoais, intenções e pensamentos. Juntas, essas migalhas contam uma história, e não é difícil predizer ações futuras das pessoas a partir desses dados. Cada vez que nos cadastramos em um novo aplicativo, que informamos nosso e-mail para uma ação promocional ou reagimos a uma publicação em redes sociais, estamos deixando uma dessas migalhas no caminho, e todas elas estão sendo recolhidas e armazenadas.

Para além do objetivo oficial com que esses dados foram coletados, muitas vezes eles são utilizados e comercializados para outras finalidades, sem nosso conhecimento ou consentimento. As consequências disso vão desde uma enxurrada de publicidade e invasão de privacidade até fraudes e manipulação de opinião. Quanto menos conscientes estivermos sobre o porquê e como nossos dados serão utilizados, maiores os riscos que corremos.

E por essa razão se fez necessária a criação da LGPD (Lei Geral de Proteção de Dados), para orientar e proteger a sociedade no uso de dados pessoais da população. Ela introduz muitas novidades e acompanha, numa perspectiva regulatória, uma evolução já em andamento da tecnologia e do nosso comportamento no meio digital.

Assim sendo, a Fundação Lemann e a Imaginable Futures acreditam que todo o sistema educacional tem uma grande

responsabilidade, a de não apenas zelar e usar bem os dados de seus alunos e profissionais, mas também o de educar as novas gerações para uma cidadania digital.

Esse manual introduz um primeiro passo muito importante nessa jornada. Ele deverá servir como referência de cabeceira para gestores educacionais conhecerem as mudanças introduzidas pela LGPD e agirem de forma prática e estruturada para a adequação de suas escolas e sistemas de ensino. Esperamos que este guia produzido de forma inovadora pelo CIEB e pelos escritórios Rennó Penteado Sampaio Advogados e Pereira Neto | Macedo Advogados sirva de apoio nessa importante trajetória.

Desejamos a todos uma boa leitura, reflexão e ação!

Lucas Machado Rocha
Gerente de Inovação na Fundação Lemann

01.

INTRODUÇÃO

O Manual de Proteção de Dados Pessoais para Gestores e Gestoras Públicas Educacionais é fruto de uma cooperação entre o Centro de Inovação para a Educação Brasileira (CIEB) e a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), com apoio da Fundação Lemann e Imaginable Futures. A publicação contou com o trabalho dos escritórios Rennó Penteado Sampaio Advogados e Pereira Neto | Macedo Advogados.

A experiência do CIEB, organização da sociedade civil que apoia as redes públicas de ensino básico a realizar uma transformação sistêmica nos processos de aprendizagem, gerando mais qualidade para a educação por meio do uso eficaz das tecnologias digitais, com o conhecimento e experiência dos parceiros envolvidos na elaboração do manual, resultam em um documento completo e em linguagem acessível, para atender gestores e gestoras públicas educacionais e oferecer orientações inéditas sobre proteção de dados pessoais no contexto da educação pública brasileira.

O desenvolvimento do Manual ocorreu em meio a um contexto de preocupação crescente com a proteção de dados pessoais no Brasil. Isso se deve, em um primeiro momento, à publicação da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD), que estabelece uma série de requisitos para que o uso de dados pessoais – inclusive nas relações de ambientes de ensino público – seja feito de maneira mais adequada. Além disso, o isolamento social, decorrente da crise de Covid-19, implicou um aumento considerável do uso de tecnologias de ensino que utilizam dados pessoais. Assim, a preocupação com um uso apropriado dos dados pessoais se tornou parte do cotidiano.

A LGPD, inclusive, insere-se em um movimento global em que o direito à privacidade se reconfigura para contemplar também a capacidade de indivíduos exercerem maior grau de controle sobre o fluxo de suas informações pessoais. Embora as primeiras normas relacionadas à proteção de dados pessoais tenham sido editadas na Europa na década de 1970, a aprovação da Convenção 108 do Conselho da Europa, em 1981, e a publicação da *General Data Protection Regulation* ("GDPR"), em 2018, iniciaram verdadeiro movimento global de aprovação de normas destinadas à proteção de dados pessoais. De acordo com levantamento da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), até o momento, 132 países já possuem leis que buscam garantir a proteção dos dados pessoais.[1]

Vale ressaltar que a redação da LGPD foi fortemente inspirada na GDPR, atualmente considerada um dos modelos regulatórios mais completos a nível global em termos de proteção de dados, de modo que boa parte das leis de proteção de dados vigentes no mundo possui influência desse modelo regulatório europeu.

Assim, os objetivos central da LGPD e das demais leis nacionais de proteção de dados se voltam a reconhecer maior autonomia e controle aos indivíduos quanto aos seus dados pessoais, por meio da imposição de obrigações aos agentes de tratamento de dados, garantindo direitos aos titulares de dados e assegurando mais transparência sobre os usos de dados. A publicação da LGPD, portanto, se situa nesse contexto, observando as boas práticas já estabelecidas e incluindo o Brasil nesse debate a nível internacional.

1 UNCTAD. Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Acesso em: 10.09.2020.

Este Manual é direcionado a gestoras e gestores públicos educacionais, e foi desenvolvido com base em atividades que realizam ou poderão realizar durante o exercício das suas funções.

Por meio de uma linguagem acessível e usando como base exemplos práticos do cotidiano da gestão pública educacional, o Manual apresenta as principais questões da LGPD, ilustrando qual o seu impacto durante o ciclo de vida do dado pessoal e indicando algumas diretrizes que devem ser consideradas para buscar a adequação a essa lei também na contratação de tecnologias educacionais. Além disso, o Manual apresenta também diretrizes voltadas ao uso de dados pessoais de crianças e adolescentes, e à adoção das cautelas necessárias tendo em vista esse público-alvo.

O Manual introduz uma breve apresentação da interface entre dados pessoais no contexto da educação pública, com enfoque especial para a aplicação da LGPD a esse setor. Em seguida, são apresentados alguns cuidados a serem observados pela gestão pública educacional na realização de atividades que envolvam dados pessoais (como coleta, utilização, transferência, armazenamento, dentre outras atividades que compreendem o conceito de tratamento de dados pessoais, conforme aprofundado mais adiante) durante todo o seu ciclo de vida e, por fim, algumas medidas que podem contribuir com a governança e as boas práticas no tratamento desses dados.

02.

QUAL A IMPORTÂNCIA DE SE FALAR EM DADOS PESSOAIS NO CONTEXTO DA EDUCAÇÃO

Na prestação de serviços de educação, sejam eles públicos ou privados, o uso de dados pessoais sempre foi frequente, como no acompanhamento e avaliação de estudantes (por meio de registros de presença, notas e condições de saúde, por exemplo), na avaliação de desempenho de docentes e demais profissionais do serviço público e no desenho de políticas educacionais. Portanto, o uso desses dados é fundamental para que os serviços educacionais possam ser prestados de maneira adequada.

Ao longo dos anos, houve um aumento considerável no uso de tecnologias digitais para apoiar práticas pedagógicas e promover inclusão digital de estudantes – por exemplo, com a aquisição de novos *hardwares* (como computadores e tablets) ou a utilização de aplicativos, sites e outras tecnologias que poderão apoiar os processos de ensino-aprendizagem e/ou a gestão da rede de ensino.[2]

A adoção dessas tecnologias[3] resulta em aumento massivo na geração de dados, bem como na capacidade de extraí-los de suas fontes e de gerar análises diversas. Alguns exemplos são:

- Aplicativos de elaboração de tarefas coletam e guardam informações como textos feitos por estudantes, forma em que realizam as tarefas, tempo gasto e/ou avaliação da atividade.
- O Censo Escolar anual do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) reúne diversas informações sobre o perfil dos(as) estudantes da rede pública no Brasil como renda, classe social, raça/cor, se é pessoa com deficiência, dentre outros.

[2] O CIEB desenvolve uma série de materiais e documentos de referência que apoiam redes de ensino e professores na adoção e uso de novas tecnologias. Dentre os exemplos podemos mencionar as práticas pedagógicas inovadoras mediadas pelo uso de tecnologia (https://cieb.net.br/o-papel-das-praticas-pedagogicas-inovadoras-mediadas-por-tecnologia/#:~:text=S%C3%A3o%20seis%20os%20modelos%20de,ensino%20h%C3%ADbrido%3A%20rota%C3%A7%C3%A3o%20por%20esta%C3%A7%C3%B5es). Outras publicações e documentos podem ser acessados no site do CIEB: https://cieb.net.br/.

[3] Para fins ilustrativos, de acordo com a Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil – TIC Kids Online Brasil 2018, 74% dos usuários de internet de 9 a 17 anos contemplados pela pesquisa utilizaram a internet para fazer trabalhos escolares. Cf. CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil – TIC Kids Online Brasil 2018. Disponível em: https://www.cetic.br/pt/tics/kidsonline/2018/criancas/B1A/. Acesso em: 14.09.2020.

Esses dados podem representar uma oportunidade para formuladores e formuladoras de políticas públicas, que podem usá-los para entender melhor as dinâmicas pedagógicas, além de integrá-los a outras fontes de informações de forma a obter importantes conclusões e fundamentar decisões direcionadas a melhorar o ensino.

No entanto, é necessário que esse uso de dados no contexto educacional seja realizado com cautela, pois a atividade pode trazer riscos consideráveis às crianças e jovens e demais envolvidos na prestação do serviço público educacional.

Isso se dá especialmente quando os titulares de dados são crianças e adolescentes. Por estarem em período de formação, esse público tende a estar menos ciente dos riscos, consequências e cautelas relacionados ao uso dos seus dados pessoais.[4] Por essa razão, são mais suscetíveis a exposições indevidas, mensagens enganosas ou publicidade excessiva, sobretudo em um contexto de maior inserção de tecnologias no seu cotidiano, tanto para as atividades educacionais quanto para o lazer.

Entre os possíveis riscos associados estão o uso inadequado ou a ocorrência de vazamentos de dados pessoais, que poderão ser, posteriormente, utilizados para a prática de crimes diversos por terceiros.

4 Internetlab. "Lei Geral de Proteção de Dados e a tutela dos dados pessoais de crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais". Disponível em: https://bit.ly/33BvJQy. Acesso em: 28.07.2020.

- Por exemplo, há o risco de discriminação gerada no uso desses dados pessoais, em casos como seleção de alunos e alunas por análises automatizadas e/ou reconhecimento facial no ambiente escolar.
- Em decorrência de incidentes de segurança da informação (ex.: vazamento de dados ou acesso indevido a dados pessoais), também é possível que sejam cometidos crimes como a fraude de identidade ou o uso de dados por terceiros para abertura de crediários em lojas.

Além disso, o contexto atual de pandemia de Covid-19 reforçou a necessidade de implementação de estratégias de aprendizagem remota, a fim de assegurar o ensino.[5] Muitas dessas estratégias envolvem o uso de tecnologias digitais e a coleta e uso de dados pessoais de estudantes, docentes e demais envolvidos. As redes de ensino precisaram se adequar rapidamente à nova realidade, especialmente quando a utilização de tecnologias educacionais é feita sem um planejamento adequado ou análise prévia em relação à maneira como são utilizados os dados do corpo de estudantes.[6]

Neste sentido, destaca-se a pesquisa "Planejamento das Secretarias de Educação do Brasil para Ensino Remoto", elaborada pelo CIEB em parceria com Consed, Undime e Fundação Lemann (publicada em abril) para avaliar a aprendizagem em tempos de isolamento social.[7]

[5] Neste sentido, o CIEB vem publicando uma série de materiais e ferramentas para apoiar gestores e gestoras públicas educacionais no contexto da pandemia de COVID-19, que podem ser acessados em: https://pandemia.cieb.net.br/. Além disso, o CIEB desenvolveu o "Guia de Implementação de Estratégias de Aprendizagem Remota", com orientações sobre como adotar estratégias de aprendizagem remota nas redes públicas de ensino para dar continuidade às aulas, promover o ensino híbrido e ampliar as oportunidades de aprendizagem dos estudantes, disponível em: https://aprendizagem-remota.cieb.net.br/guia.

[6] Em vista dos riscos quanto ao uso de tecnologias sem prévia avaliação sobre como as ferramentas coletam e usam os dados durante o contexto da pandemia de Covid-19, o Estado do Rio de Janeiro publicou a Lei nº 8.973/2020 que proíbe o uso de dados pessoais, dados pessoais sensíveis e metadados de usuários de plataformas virtuais de ensino à distância para fins de exploração comercial. Essa iniciativa se dá em relação às ofertas gratuitas de tecnologias para instituições de ensino utilizarem durante a pandemia. Disponível em: https://www.legisweb.com.br/legislacao/?id=399821. Acesso em 30.07.2020.

[8] CIEB. "Pesquisa: Planejamento das Secretarias de Educação do Brasil para Ensino Remoto". Disponível em: https://cieb.net.br/wp-content/uploads/2020/04/CIEB-Planejamento-Secretarias-de-Educac%C3%A3o-para-Ensino-Remoto-030420.pdf. Acesso em 30.07.2020.

De fato, além dos potenciais riscos impostos aos(às) titulares de dados, o uso inadequado de dados pessoais pode gerar danos à rede de ensino, à gestão pública e/ou a terceiros que estejam envolvidos na prestação de serviços de educação (ex.: empresas fornecedoras de *softwares*). Esses riscos são variados e abrangem a imposição de multas, prejuízos para a imagem da rede de ensino e riscos aos(às) titulares de dados, especialmente aos(às) estudantes.

Diante desse contexto e da crescente adoção de tecnologias nos processos de ensino-aprendizagem, é crucial que a prestação do serviço público educacional esteja também preocupada com a proteção dos dados pessoais. Isso é importante tanto para que gestores e gestoras possam melhor direcionar esforços e recursos no desenho e execução de políticas públicas educacionais, quanto para assegurar direitos de alunos e alunas, professores e professoras e demais envolvidos no sistema de ensino (ex.: familiares e responsáveis, diretores e diretoras escolares, etc.). Além disso, a implementação de tecnologias nos serviços públicos de educação devem ser adequadas em termos de tratamento de dados pessoais, reforçando a segurança e confiança da população no seu uso.

Por isso, este Manual esclarece alguns conceitos importantes e fornece orientações sobre como usar adequadamente dados pessoais na área da educação.

03.

COMO A LEI GERAL DE PROTEÇÃO DE DADOS SE APLICA AO SETOR EDUCACIONAL?

01.

QUAL O OBJETIVO DE UMA LEI DE PROTEÇÃO DE DADOS?

Leis de proteção de dados vêm sendo publicadas em diversos países com o objetivo de trazer maior proteção às pessoas cujos dados são usados, e oferecer maior segurança jurídica para as empresas ou pessoa que utilizam esses dados.

No Brasil, o uso de dados pessoais, por entidades públicas ou privadas, – em documentos físicos ou digitais – é abordado pela Lei n° 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD).

O objetivo da LGPD é fazer com que os dados pessoais sejam usados de forma a não afetar direitos de pessoas que estejam no Brasil (incluindo pessoas estrangeiras que estejam no país).

A LGPD se aplica às atividades do sistema de ensino sempre que houver o uso de dados pessoais (ex.: desde o momento de pedido de vagas em escola, passando pela permanência dos alunos e alunas e até mesmo após a sua saída, nos casos em que for

permitido/requerido o armazenamento desses dados, além daqueles relacionados aos responsáveis legais, docentes, gestores e gestoras e demais envolvidos na prestação dos serviços).

02.

O QUE SÃO DADOS PESSOAIS?

O dado pessoal é qualquer informação **que identifique ou permita identificar uma pessoa natural (chamada de "titular de dados").**

O(a) titular dos dados é a pessoa a quem se referem os dados pessoais. No contexto educacional, os(as) titulares geralmente são **estudantes, representantes legais, docentes, servidoras e servidores públicos da escola, equipe de coordenação, diretores e diretoras escolares, entre outros.**

EXEMPLO DE DADOS PESSOAIS DE ESTUDANTES ☒

1. identidade, histórico escolar, informações médicas, endereço, telefone, e-mail, carteira estudantil, registro de aluno/a (RA), Número de Identificação Social (NIS), informações sobre necessidades especiais; ou

2. informações geradas no uso de tecnologias e que permitam identificar os alunos e alunas, como a gravação de imagens por câmeras de segurança, as análises geradas pelo uso de aplicativos educacionais, a coleta do IP do dispositivo móvel utilizado.

OK

EXEMPLOS DE DADOS DE FAMILIARES E RESPONSÁVEIS ☒

Renda, situação civil (ex.: casado/a, divorciado/a, falecido/a, etc), telefone, endereço, e-mail, escolaridade, relatórios de reuniões, assinaturas, NIS, etc.

OK

EXEMPLOS DE DADOS DE DOCENTES E DEMAIS SERVIDORAS E SERVIDORES PÚBLICOS

1. identidade, idade, profissão, currículo, avaliação de desempenho, endereço, telefone, e-mail, salário;

2. informações geradas no uso de tecnologias e que permitam identificar essas pessoas, como a gravação de imagens por câmeras de segurança ou videoaulas, as análises geradas pelo uso de aplicativos educacionais, a coleta do IP do dispositivo móvel utilizado.

OK

Os **dados pessoais sensíveis**, por sua vez, são informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Esses dados requerem cuidados diferenciados por se referirem às esferas mais íntimas e pessoais e por darem margem a tratamentos discriminatórios.

EXEMPLOS DE DADOS SENSÍVEIS DE ALUNOS E ALUNAS ☒

Informações médicas (distúrbios e restrições alimentares), religião e dados biométricos para acesso à escola. Imagens serão consideradas dados sensíveis se utilizadas para realizar inferências sobre dados sensíveis, como raça/cor.

OK

EXEMPLOS DE DADOS SENSÍVEIS DE DOCENTES ☒

Marcações sobre raça/cor, informações médicas, opinião política ou filiação a sindicato.

OK

EXEMPLOS DE DADOS SENSÍVEIS DE RESPONSÁVEIS LEGAIS ☒

Religião, dados médicos, vinculação a partido político ou sindicato.

OK

Vale ressaltar que a LGPD também traz requisitos específicos para o tratamento de **dados pessoais de crianças e adolescentes**.

De acordo com o Estatuto da Criança e do Adolescente ou ECA (Lei nº 8.069/1990), lei que busca resguardar a proteção aos menores no país, considera-se **criança** a pessoa com até 12 anos de idade; já **adolescente** é aquela que possui entre 12 e 18 anos de idade.

Em relação aos dados pessoais sensíveis, os dados pessoais de menores também demandarão maiores cuidados ao longo do seu uso.

EXEMPLOS DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES ☒

` Dados de cadastro de alunos(as) do ensino infantil; indicadores de performance escolar de adolescentes.

OK

03.

COMO SE CHAMAM AS OPERAÇÕES REALIZADAS COM DADOS PESSOAIS?

De acordo com a LGPD, qualquer atividade realizada com dado pessoal é chamada de **tratamento**. Isso envolve, por exemplo, coleta, utilização, acesso, transferência, modificação, análise, armazenamento e eliminação de dados pessoais.

Assim, na prática, qualquer uso de dados pessoais será considerado uma atividade de tratamento de dados pessoais.

Além disso, o tratamento de dados não está apenas relacionado ao uso de dados em formato digital (por exemplo, em plataformas educacionais ou ferramentas de avaliação estudantil), mas também ao uso de dados disponibilizados em formato físico (por exemplo, fichas cadastrais em papel e listas de presença).

Por conta disso, gestores e gestoras educacionais e equipes de educação devem avaliar quais são os tipos de atividades de tratamento realizadas normalmente no ambiente escolar (os cuidados necessários em relação a essas atividades serão abordados mais adiante neste Manual). Alguns exemplos:

EXEMPLOS

No decorrer das práticas escolares são realizadas diversas atividades com dados pessoais, tais como: realizar a matrícula dos alunos e alunas, realizar o controle de presença, emitir boletins, elaborar relatórios de desempenho, armazenar históricos escolares, gravar imagens por câmeras de segurança, entrar em contato com estudantes e familiares, realizar procedimentos de saúde quando necessário, dentre outras.

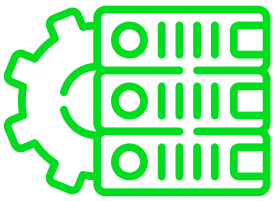
Também são atividades de tratamento de dados pessoais a comunicação de dados de um aluno ou aluna para outra instituição de ensino ou para secretarias de educação, municipais ou estaduais, ou outras entidades públicas.

Além disso, a escola e/ou rede de ensino também realiza o tratamento de dados de estudantes com o uso de ferramentas digitais, como a realização de atividades e avaliações com programas ou aplicativos, armazenamento de informações em sistemas computacionais da escola, utilização de e-mail para comunicação com familiares ou responsáveis, entre outras atividades.

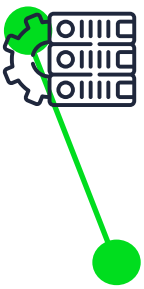
É importante já adiantar que qualquer atividade de tratamento de dados realizada com crianças e adolescentes deve ser realizada para atender ao seu melhor interesse, em consonância com o ECA. Em termos de proteção de dados, o melhor interesse significa que qualquer atividade de tratamento deve ser pautada pela proteção e cuidado dos menores e em seu próprio benefício.

OK

04.



QUEM SÃO AS PARTES ENVOLVIDAS NAS ATIVIDADES DE TRATAMENTO DE DADOS?



Além de entender o que são dados pessoais e quais são as atividades de tratamento de dados pessoais, é importante esclarecer outros conceitos da LGPD que permitem identificar os(as) envolvidos(as) no uso desses dados. São eles:

Controlador(a)

Operador(a)

Encarregado(a)

Quem é controlador(a) e quem é operador(a) dos dados pessoais?

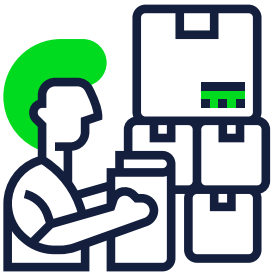
Controlador(a)

1. Por definição, é quem toma as decisões sobre como serão usados os dados pessoais.

2. No contexto escolar, as escolas, secretarias municipais e estaduais de educação podem ser exemplos dessa figura, na medida em que possuem atribuição legal para decidir como serão executadas as políticas de educação (e, consequentemente, quais serão os dados pessoais pertinentes para serem utilizados e como serão utilizados).

Operador(a)

1. É quem realiza o tratamento de dados segundo as instruções fornecidas pelo controlador ou controladora, não podendo usar os dados para outras finalidades fora dessas instruções.



Exemplo 1: uma secretaria de educação contrata uma empresa para fornecer às escolas da rede pública municipal câmeras de segurança e infraestrutura de armazenamento das imagens gravadas. Entre os requisitos do contrato, a secretaria indica onde serão instaladas as câmeras, quem pode ter acesso às filmagens e por quanto tempo as filmagens devem ser armazenadas (toma decisão sobre o tratamento). Entretanto, quem realiza a gravação e armazena as imagens é a empresa contratada (realiza o tratamento de dados em nome do controlador). Neste exemplo, a secretaria é a controladora e a empresa, a operadora.

Exemplo 2: a secretaria de educação de determinado município contrata uma ferramenta de gestão escolar para as escolas do município. A ferramenta compreende a guarda, o armazenamento e o processamento de diversos dados custodiados pelas instituições como: históricos escolares, fichas médicas, contatos de docentes, contato de alunos e alunas e responsáveis, entre outros. A secretaria estabelece um contrato com o desenvolvedor ou desenvolvedora da ferramenta e estabelece que é sua função armazenar as informações em sua plataforma, vetando, portanto, o uso desses dados.

2. Vale ressaltar que as pessoas físicas que tenham acesso aos dados pessoais devido à sua condição profissional na instituição de ensino ou na própria administração pública (como o corpo docente, as diretorias e o funcionalismo do setor administrativo) não são considerados operadores ou operadoras de acordo com a LGPD.

OBSERVAÇÃO

Nem todas as atividades de tratamento de dados possuem um(a) controlador(a) e um(a) operador(a). Na grande maioria dos casos, há apenas o(a) controlador(a) dos dados, que toma a decisão sobre o tratamento desses dados e realiza o seu tratamento. No contexto educacional, esse é o caso das atividades mais corriqueiras como realizar matrícula, avaliar estudantes por meios tradicionais, etc. Entretanto, com o aumento do uso de ferramentas tecnológicas, passa a ser mais comum a existência também do operador ou operadora dos dados. Normalmente, quem fornece o produto ou desenvolve a ferramenta é quem realiza atividades de tratamento, como armazenamento e processamento de dados para a funcionalidade de sua ferramenta.

OK

Quem é o encarregado ou a encarregada?

Encarregado (a)

1. É a pessoa indicada para atuar como canal de comunicação entre a secretaria e as escolas, os(as) estudantes, docentes e outros titulares dos dados e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

> A ANPD é a autoridade com capacidade de, entre outras atribuições legais, regular, realizar consultas e fiscalizar o cumprimento da LGPD.

2. Suas atividades consistem em aceitar reclamações de titulares dos dados, prestar esclarecimentos, receber denúncias, adotar providências, orientar o funcionalismo público a respeito de práticas de tratamento de dados, dentre outras.

3. Para desenvolver suas tarefas de maneira adequada, esse(a) profissional deve possuir qualificações apropriadas, tais como[8]:

[8] Estas recomendações são baseadas em entidades europeias de proteção de dados pessoais, com base na interpretação do regulamento europeu de proteção de dados, a GDPR. Vale ressaltar que a GDPR, considerada uma das legislações mais completas em termos de proteção de dados pessoais, serviu de inspiração para a redação da LGPD, e pode inclusive vir a ser observada pela ANPD para fins de interpretação da lei brasileira. ICO (Information Comissioner's Office. "WP29 Guidelines on Data Protection Officers ("DPOs"); ICO Data protection officers". Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/. Acesso em 01.09.2020.

A. Conhecimento aprofundado sobre a LGPD;

B. Compreensão das operações de tratamento de dados pessoais realizadas pela **secretaria de educação**;

C. Bom trânsito com a área de tecnologia da informação e segurança de dados do órgão ou entidade;

D. Capacidade de diálogo com autoridades com competência para fiscalizar atividades de proteção de dados pessoais; e

E. Habilidade de promover uma cultura de proteção de dados pessoais dentro do órgão público.

OBSERVAÇÃO

Nem sempre será necessário nomear um encarregado ou uma encarregada para cada órgão da administração pública. Por exemplo, uma prefeitura de menor porte pode, a depender das circunstâncias, nomear apenas uma pessoa nessa área para todos os seus órgãos ou entidades. Essa decisão vai depender do tamanho da administração pública (nesse exemplo, municipal) e dos recursos disponíveis. Idealmente, tendo em vista que órgãos ou entidades públicas podem realizar atividades muito distintas entre si, é recomendável que cada um possua seu próprio encarregado ou encarregada.

OK

SAIBA MAIS

Mais informações sobre o(a) encarregado(a), como nomeá-lo(a), e quais os pontos de atenção na sua atuação serão abordadas no tópico: **“Recomendações e boas práticas”**.

05.

QUAIS SÃO OS PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS NA LGPD?

A proteção aos dados oferecida pela LGPD tem como base dez princípios. São eles:

1. Finalidade

Considerado um dos mais relevantes para a interpretação da lei, esse princípio exige que todos os usos e operações realizadas com dados pessoais devem ser feitos para propósitos determinados, legítimos e específicos, e conforme as finalidades informadas ao(à) titular de dados. Em outras palavras, o princípio da finalidade determina que o tratamento de dados nunca deve ser genérico, mas, sim, ser feito para uma finalidade específica.

Exemplo 1: quando são coletadas imagens de estudantes no ambiente escolar por meio de câmeras, a finalidade é garantir sua segurança. A princípio, essa finalidade parece legítima, uma vez que é realizada em benefício das crianças e jovens. No entanto, caso essas imagens sejam compartilhadas com outras empresas ou organizações para outras finalidades distintas das informadas aos(às) titulares de dados, é possível que haja riscos no uso desses dados.[9]

Exemplo 2: a diretoria de uma escola disponibiliza uma lista com dados de contato dos(as) responsáveis legais de determinadas estudantes para uma pessoa de sua família, que possui uma loja de artigos infantis, de modo que ela possa oferecer ofertas para esse público. Essa disponibilização de dados pode violar o princípio da finalidade na medida em que os dados serão utilizados para finalidades distintas e não compatíveis com aquelas que foram informadas aos(às) titulares durante a sua coleta.

[9] Commission Nationale de l'Informatique et des Libertés (CNIL). "Vigilância por vídeo: proteção de dados pessoais nas escolas". Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaires. Acesso em: 24.07.2020.

2. Adequação

Esse princípio exige que haja compatibilidade entre a atividade de tratamento dos dados pessoais realizada e as finalidades informadas ao(à) titular de dados, de acordo com o contexto do tratamento.

Exemplo: Uma instituição de ensino coleta dados de contato dos(as) estudantes para se comunicar com eles e com seus responsáveis. Todavia, compartilham esses dados (sem informar os/as titulares) com uma escola de idiomas a fim de que esta possa oferecer seus serviços. Nesse caso, a atividade extrapola as finalidades e informações prestadas ao(à) titular de dados.

3. Necessidade

Segundo esse princípio, o tratamento dos dados deve ser limitado ao necessário para a realização de suas finalidades. Isso quer dizer que, nas operações realizadas com dados pessoais, as entidades devem se certificar de que estão usando apenas os dados necessários para cumprir a finalidade pretendida.

De acordo com esse princípio, não é possível coletar dados sem uma finalidade específica apenas com a justificativa de que eles poderão ser úteis no futuro.

Exemplo: uma **secretaria de educação** quer fazer um estudo sobre a relação entre a distância da residência dos(as) estudantes para a escola e seu comparecimento nas aulas. Para isso, solicita que as escolas compartilhem endereço e informações de presença dos(as) estudantes. Entretanto, a escola compartilha, além desses dados, informações adicionais, como telefone dos familiares e histórico escolar – o que não seria necessário para o alcance da finalidade pretendida.

4. Livre acesso

Esse princípio assegura a consulta facilitada e gratuita sobre as formas e duração das operações realizadas com dados pessoais. Isso significa que cidadãos e cidadãs têm a prerrogativa de acessar os seus dados pessoais de forma livre, irrestrita e gratuita, de modo que este princípio também figura como fundamento de vários dos direitos na LGPD.

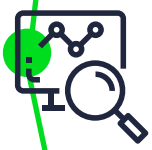
Exemplo: Caso um estudante formado deseje saber quais dados ainda são mantidos a seu respeito, a escola ou rede de ensino deve ser capaz de fornecer informações completas, justificar a duração das operações realizadas e o motivo do armazenamento.

5. Qualidade dos dados

Esse princípio exige a garantia de exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade do seu uso e para o cumprimento da finalidade pretendida. Isso deve ser levado em conta porque eventuais informações imprecisas podem prejudicar direitos e interesses do(a) titular dos dados.

Exemplo: O uso de dados de estudantes que estejam incorretos pode prejudicar a concessão de benefícios, como auxílios de transporte não concedidos em decorrência de cadastro de endereço desatualizado.

6. Transparência



Segundo esse princípio, é necessário prestar informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Embora certas informações sobre o tratamento de dados pessoais de crianças e adolescentes possam ser destinadas aos seus familiares/responsáveis legais, é necessário que esse princípio seja exercido também em relação aos menores. Isso deve ocorrer, por exemplo, por meio do uso de vocabulário, tom e estilos apropriados para esse público-alvo, de modo que os menores possam compreender a mensagem.

Exemplo: Órgãos públicos educacionais devem abordar em suas políticas de transparência esclarecimentos sobre como usam dados pessoais de estudantes, docentes, servidores e servidoras públicas de escolas.

7. Não discriminação

O princípio da não discriminação diz respeito à impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos. Esse princípio busca assegurar que os dados pessoais não serão usados para finalidades que envolvam segregação social, racial ou de gênero.

Quando o tratamento envolver dados de crianças e adolescentes, deverão também ser observadas as disposições do ECA, segundo o qual crianças e adolescentes devem ser tratados sem discriminação em relação à situação familiar, idade, sexo, raça, etnia, religião, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, local de moradia, dentre outras condições de diferenciação entre os menores.

Exemplo: Não seria possível, no contexto da pandemia de Covid-19, que uma escola utilizasse dados sensíveis de estudantes para excluir os portadores de deficiências do retorno às atividades presenciais – dado que, em alguma medida, poderia se entender que a decisão deriva de uma equiparação entre deficiência e comorbidade. Nesse caso, ocorreria uma violação ao direito da não discriminação nos termos da LGPD, tendo em vista que o uso de dados possibilitaria uma medida de exclusão.

8. Segurança

Esse princípio exige o uso de medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Exemplo: Uma escola ou secretaria possui uma plataforma própria de disponibilização das notas dos(as) estudantes, contendo também outros dados, tais como identidade e informações documentais. No entanto, por falha de segurança na plataforma, os dados referidos ficaram com acesso irrestrito, permitindo que pessoas não autorizadas os analisassem sem exigência de *login* e senha. Essa situação representa uma violação ao princípio da segurança.

9. Prevenção

Esse princípio se refere à adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. A questão do *privacy by design* – ou seja, a inclusão da preocupação com proteção de dados desde a concepção de um projeto – está relacionada com esse princípio.

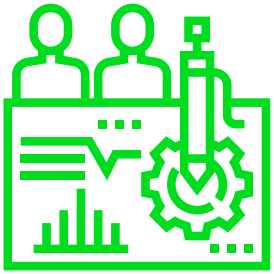
Exemplo: Uma forma de cumprir o princípio da prevenção seria, por exemplo, a utilização de *login* e senha individuais com procedimento de dupla autenticação para cada estudante em plataforma *online* disponibilizada pela escola ou secretaria. Isso dificultaria o acesso indevido e preveniria danos. Esse mesmo procedimento, inclusive, poderia ser adotado em outras situações a fim de impedir acesso a pessoas não autorizadas em sistemas e bases de dados internas da escola ou secretaria.

10. Responsabilização e prestação de contas (*accountability*)

Por fim, o princípio da responsabilização e prestação de contas (*accountability*) envolve a demonstração 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 1: Uma forma de cumprimento desse princípio está na disponibilização, pela escola ou pela secretaria, de informações básicas a respeito das medidas de segurança da informação adotadas no tratamento de dados.

Exemplo 2: Outra medida nesse sentido seria a realização de estudos para fins de análise dos impactos e riscos envolvendo os tratamentos de dados pessoais realizados durante as atividades escolares.



06.

QUANDO A SECRETARIA OU ESCOLA PODEM TRATAR DADOS PESSOAIS?

Com a entrada em vigor da LGPD, é comum imaginar que, a partir de agora, só será possível utilizar dados pessoais com base no consentimento do(da) titular. Entretanto, esse entendimento não é correto. Na realidade, o consentimento é só uma das dez hipóteses que a LGPD permite tratar dados pessoais.

Esse é um dos pontos mais importantes da LGPD: o estabelecimento das **bases legais para o tratamento de dados pessoais**.

Em linhas gerais, as bases legais são as hipóteses previstas na lei que autorizam o tratamento de dados pessoais. Essas hipóteses, por sua vez, podem ser diferentes a depender do tipo de dado – isto é, dado pessoal ou dado pessoal sensível.

A tabela abaixo identifica essas hipóteses:

DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS
Mediante o fornecimento de consentimento pelo(a) titular	Mediante o fornecimento de consentimento pelo(a) titular
Cumprimento de obrigação legal ou regulatória;	Cumprimento de obrigação legal ou regulatória;
Pela administração pública, para o tratamento de dados necessários à execução de políticas públicas previstas em leis, regulamentos e contratos;	Pela administração pública, para o tratamento de dados necessários à execução de políticas públicas, previstas em leis e regulamentos;
Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
Para execução de contrato ou procedimentos preliminares ao contrato;	Para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
Exercício regular de direitos em processo judicial, administrativo ou arbitral;	Para proteção da vida ou da incolumidade física do(a) titular ou de terceiros;
Para proteção da vida ou da incolumidade física do(a) titular ou de terceiros;	Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;	Garantia da prevenção à fraude e à segurança do(a) titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.
Quando necessário para atender aos interesses legítimos do(a) controlador(a) ou de terceiro; ou	
Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	

Como gestor ou gestora educacional, o importante é identificar quais dessas bases legais se aplicam às atividades de tratamento de dados realizadas no âmbito das secretarias de educação e do ensino público. Ao menos uma dessas hipóteses deve se aplicar quando se realiza atividade de tratamento de dados pessoais.

Vale ressaltar ainda que, de acordo com a LGPD, o **tratamento de dados pessoais não necessariamente precisa do consentimento do(a) titular para ser considerado lícito** – desde que apresente outra base legal mais adequada. Em especial, para o setor público, existe uma série de outras hipóteses ou bases legais mais adequadas para viabilizar esse tratamento.

Abaixo, **identificamos as principais bases legais aplicáveis ao seu cotidiano, enquanto gestora ou gestor público na área da educação**, e fornecemos alguns exemplos que podem ajudar a realizar essa identificação para outras atividades.

01. Tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória:

Com essa base legal, a LGPD quer dizer que secretarias ou escolas podem usar dados pessoais nas suas atividades, desde que esses dados sejam necessários para o cumprimento de uma lei ou norma.

Exemplo 1: A Constituição Federal determina que o Poder Público deverá recensear educandos no ensino fundamental, fazer-lhes a chamada e zelar, junto aos familiares ou responsáveis, pela frequência à escola (art. 208, §3°), o que envolve o tratamento de uma vasta quantidade de dados pessoais.

Exemplo 2: A Resolução nº 1 de 2018 CNE/MEC exige que sejam coletados diversos dados pessoais de estudantes, como nome, filiação, raça/cor, etnia, deficiência, entre outros, com a finalidade de realizar o censo escolar pelo INEP.

Exemplo 3: Resoluções expedidas pelas secretarias de educação dos estados e municípios estabelecendo os dados necessários para realização de matrícula na rede pública também implicam o uso de grande quantidade de dados pessoais.

02. Tratamento e uso compartilhado de dados pessoais necessários à execução de políticas públicas:

Essa hipótese de tratamento abrange diversas atividades realizadas por órgãos públicos na consecução de suas atividades. Isso envolve o uso compartilhado de dados para execução de diversas políticas públicas, tais como políticas assistenciais no setor educacional, políticas relacionadas ao transporte escolar, políticas de representatividade, dentre outras.

Exemplo: Secretaria de educação compartilha dados de estudantes da educação básica, como nome, endereço e filiação, com a secretaria de transportes para viabilizar a elaboração de políticas públicas de transporte escolar.

03. Tratamento de dados pessoais necessário para a execução de contrato:

Essa base legal se aplica nos casos em que o tratamento de dados pessoais for necessário para a execução de determinado contrato (ou de procedimentos preliminares a esse contrato). No entanto, essa base legal se aplica aos contratos celebrados com o(a) titular de dados e envolve apenas os dados pessoais necessários para que os contratos sejam celebrados. Além disso, vale ressaltar que essa base legal se refere apenas a contratos que têm como uma de suas partes o(a) titular dos dados pessoais que são tratados.

- **Exemplo 1:** contrato de trabalho firmado entre secretarias de educação e docentes da educação básica. Normalmente, exigem que sejam coletados dados pessoais dos docentes.

- **Exemplo 2:** tratamento de dados de docentes – como nome completo, filiação, endereço, dentre outros – para fins de celebração de contrato por prazo determinado.

04. Tratamento de dados pessoais mediante consentimento do(a) titular:

O consentimento é uma manifestação (deverá envolver uma ação específica de aceite – ex.: caixa de seleção não previamente marcada) do(a) titular na qual concorda que seus dados sejam usados para determinada finalidade.

No contexto do sistema público de educação, o consentimento será uma base legal secundária, ou seja, aplicável apenas quando não for possível fundamentar a atividade de tratamento de dados pessoais em outra base legal. Por exemplo, o consentimento pode ser necessário quando o tratamento envolver o uso de informações mais sensíveis, como imagens, fotos e biometria.

Para estudantes com mais de 12 anos (há quem argumente que isso se aplica aos maiores de 16 anos), a escola ou secretaria poderá obter o consentimento diretamente do(a) estudante, desde que a escola ou secretaria assegure que ele/a entendeu o que está consentindo.

No caso de menores de 12 anos (ou os menores de 16 anos, na visão de alguns), deverá ser obtido consentimento parental por pelo menos um dos familiares ou responsáveis.

Vale ressaltar que o consentimento parental, para além de buscar a proteção dos direitos daqueles que representa, não deve gerar prejuízos ao direito à liberdade dos menores para fins de opinião e expressão, por exemplo, como dispõe o ECA, o que envolve o seu engajamento em determinados ambientes que utilizam os seus dados pessoais (ex.: plataformas digitais que procedem com a coleta de dados pessoais desses menores).[10]

Exemplo 1: escola ou secretaria quer usar a foto de um menor de 12 anos que ganhou olimpíada de matemática para fins de publicidade. Nesse caso, é recomendável coletar o consentimento dos familiares ou responsáveis para usar essa imagem.

[10] YANDRA, Barbara Fernanda Ferreira; SILVA, Amanda Cristina Alves; SANTOS, Jéssica Guedes. Lei Geral de Proteção de Dados e a tutela dos dados pessoais de crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais. Dsiponível em: https://revista.internetlab.org.br/lei-geral-de-protecao-de-dados-e-a-tutela-dos-dados-pessoais-de-criancas-e-adolescentes-a-efetividade-do-consentimento-dos-pais-ou-responsaveis-legais/. acesso em: 10.09.2020.

Exemplo 2: compartilhamento de dados de estudantes para empresa de material escolar realizar marketing ou divulgações institucionais (não eleitorais). Nesse caso, o compartilhamento de dados com terceiro está fora do contexto ou finalidade educacional, portanto, seria necessário coletar o consentimento.

Exemplo 3: escola ou secretaria querem postar, em suas próprias redes sociais, vídeos com interações de estudantes em ambiente escolar. Nesses casos, também se recomenda a obtenção de consentimento dos familiares ou responsáveis legais.[11]

05. Tratamento de dados pessoais para exercício regular de direitos em processo judicial, administrativo ou arbitral:

Fase aplicada quando há necessidade de usar dados pessoais para defender os interesses do ente público ou da instituição em processos judiciais ou administrativos.

Exemplo: uso de dados pessoais de docentes por determinada escola para fins de produção de provas em processo judicial no qual a escola esteja

[11] BORELLI, Alessandra. "É pra já! A proteção de dados de crianças e adolescentes não pode esperar". Julho de 2020. Disponível em: https://cdn.asp.events/CLIENT_Ascentia_4E961A52_5056_B739_54289B84DF34E888/sites/BettBrasil20Port/media/E%CC%81%20pra%20ja%CC%81%20-%2025%20agosto.pdf. Acesso em: 31.08.2020.

envolvida, desde que estritamente necessário para a defesa dos seus interesses.

06. Tratamento de dados pessoais para atendimento ao legítimo interesse do controlador ou da controladora:

A base do legítimo interesse é a mais genérica da LGPD. Ela não se aplica ao tratamento de dados pessoais sensíveis, e somente poderá ser usada para tratamento de dados pessoais que buscam 1) o apoio e promoção de atividades do controlador ou da controladora; e 2) proteção aos direitos de titular e prestação de serviços que o beneficiem.

No ambiente escolar, essa base legal poderá ser usada para o tratamento de dados em atividades mais corriqueiras. No entanto, há debates sobre a possibilidade do uso dessa base legal por órgãos e entidades do poder público. Por isso, sempre que possível, recomenda-se utilizar outras bases legais mais específicas, como a execução de contrato ou de políticas públicas.

Exemplo: Entrar em contato por e-mail ou telefone com familiares ou responsáveis para informar sobre eventos que venham a ser realizados na instituição de ensino.

07.

DIREITOS DOS(AS) TITULARES DE DADOS PESSOAIS E SEU RELACIONAMENTO COM A REDE DE ENSINO

Outro aspecto fundamental na LGPD é o estabelecimento dos chamados direitos dos(as) titulares dos dados pessoais. Basicamente, esses direitos são os mecanismos legais dos quais as pessoas dispõem para ter controle sobre seus dados pessoais e exigir que eles sejam tratados em conformidade com a LGPD.

Na prática da gestão educacional, isso significa que estudantes, familiares, docentes, servidores e servidoras públicas poderão exigir das secretarias ou escolas informações e ações relacionadas às atividades de tratamento realizadas que envolvam seus dados pessoais.

Para responder a essas solicitações, entidades educacionais que realizam operações com dados pessoais devem manter estruturas (sejam elas técnicas ou de comunicação, por exemplo) para o relacionamento com os(as) titulares a respeito de

seus dados. Abaixo, sistematizamos os direitos dos(as) titulares e as ações que deverão ser feitas para atendê-los:

1. Direito de ser informado:

Estudantes, professores(as), familiares ou responsáveis legais e outros titulares têm o direito de receber informações como:

1. quais dados estão sendo coletados e processados;
2. por qual motivo estão sendo coletados;
3. com quais organizações estão sendo compartilhados; e
4. como estão sendo armazenados e por quanto tempo.

2. Direito de confirmação da existência do tratamento:

Direito de obter, a qualquer momento, a confirmação sobre a existência do tratamento de seus dados pessoais pela instituição de ensino ou pela secretaria.

Para atender a esse direito, pode-se fornecer uma resposta objetiva, com redação simples, confirmando que são tratados ou não dados pessoais relacionados ao(à) titular.

3. Direito de acesso:

O direito de acesso aos dados pessoais tratados pode ser cumprido de várias maneiras, como por meio de

visualização em telas, envio por e-mail, por escrito ou por meio de cópias físicas em que constem os dados solicitados.

Vale ressaltar que é essencial que os dados sejam transmitidos de modo inteligível, claro e adequado a fim de que o(a) titular de dados possa realmente compreender como ocorre esse tratamento.

4. Direito de correção:

Os(as) titulares podem solicitar que os seus dados sejam corrigidos quando estiverem incompletos, inexatos ou desatualizados.

O objetivo desse direito é garantir a qualidade dos dados tratados.

5. Direito de anonimização, bloqueio e eliminação de dados:

Os(as) titulares podem solicitar a eliminação, o bloqueio ou a **anonimização** de dados pessoais que sejam desnecessários, excessivos ou tratados em desconformidade com a LGPD.

Vale ressaltar que há situações em que esses dados não poderão ser eliminados, bloqueados ou anonimizados, como nos casos em que o armazenamento de dados pessoais por determinado período é solicitado por uma determinada lei.

Quando for solicitada a anonimização dos dados pessoais, recomenda-se certificar que a técnica aplicada exclua a capacidade de o dado revelar a identidade da pessoa (e, portanto, deixe de ser um dado pessoal).

Quando for solicitado o **bloqueio** dos dados pessoais (a suspensão temporária de determinadas operações de tratamento), recomenda-se verificar se há limite de acesso a determinadas áreas ou de compartilhamento dos dados com terceiros ou, ainda, em relação a uma finalidade específica aplicada ao dado em tratamento.

Quando for solicitada a **eliminação** dos dados pessoais (ou seja, exclusão definitiva dos dados pessoais), eles deverão ser excluídos dos bancos de dados da instituição de ensino e/ou **secretaria de educação**. Para cumprir essa solicitação, deve-se verificar se não há situações que justifique o tratamento/armazenamento desse dado, e se não há outras finalidades que autorizem a sua manutenção.

6. Direito de informações sobre o compartilhamento dos dados:

Os(as) titulares podem ter acesso a informações que indiquem com quais entidades públicas e/ou privadas os seus dados foram compartilhados.

7. Direito de portabilidade:

O direito à portabilidade permite que os(as) titulares obtenham e reutilizem os seus dados pessoais junto a outro agente de tratamento de dados pessoais.

Para viabilizar esse direito, recomenda-se que esses dados sejam fornecidos em um formato interoperável (por exemplo, que utilize padrões e linguagens passíveis de comunicação com outras tecnologias) de modo a permitir uma fácil utilização por parte do novo controlador ou nova controladora desses dados.

Vale ressaltar que a portabilidade não incluirá dados que já tenham sido anonimizados pelo controlador ou pela controladora.

8. Direito de eliminação dos dados tratados com base no consentimento:

Os(as) titulares têm direito de solicitar a eliminação definitiva de dados pessoais que foram tratados com base em consentimento previamente concedido.

Logo, esse direito se aplica para os casos em que o consentimento foi obtido.

9. Direito de receber informações sobre a possibilidade de não oferecer o consentimento:

De acordo com esse direito, o(a) titular pode possuir não apenas informações sobre a possibilidade de não fornecer o seu consentimento para uma determinada atividade de tratamento de dados, como também sobre as consequências de não fornecer esse consentimento.

10. Direito de revogação do consentimento:

Permite ao(à) titular revogar o seu consentimento previamente concedido a qualquer momento por meio de solicitação expressa.

Esse procedimento de revogação deve ser gratuito e facilitado – ou seja, deve ser fornecido no mesmo momento da coleta do consentimento e em demais interações com o(a) titular que envolvam o tratamento de dados.

11. Informação sobre as entidades com as quais os dados foram compartilhados

Permite ao(à) titular possuir informações sobre as entidades públicas e privadas com as quais o controlador ou a controladora compartilhou dados.

12. Direito de revisão de decisões automatizadas:

Por fim, o(a) titular pode solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

> **Exemplo:** Decisões automatizadas voltadas à criação de um determinado perfil de estudante (ex.: perfil socioeconômico gerado automaticamente).

Essa revisão pode ser realizada tanto por indivíduos quanto de maneira automatizada, pois a LGPD não impõe limitações nesse sentido.

Quem pode exercer esses direitos?

Esses direitos podem ser exercidos apenas por titulares ou por seus representantes legais.

No caso de estudantes menores de idade, seus familiares ou representantes legais poderão lhes representar no exercício desses direitos.

Se os direitos se referirem a dados pessoais dos próprios familiares ou de servidores e servidoras públicas, entende-se que eles próprios serão legitimados para exercer esses direitos.

Como esses direitos podem ser exercidos?

Os direitos dos(as) titulares e a maneira pela qual esses direitos podem ser exercidos devem ser **informados** de forma clara e adequada.

Esses direitos serão exercidos por meio de **requerimento expresso** do(a) titular ou de seu representante legal, **sem qualquer custo ao(à) titular.**

Como esses direitos podem ser viabilizados?

Para viabilizar o exercício desses direitos, uma recomendação é a criação de um **canal de interação**, como um endereço de e-mail ou ramal próprio para esclarecer questões relacionadas à proteção de dados. Alternativamente, podem ser fornecidos um link ou uma seção específica no site para atendimento das demandas.

Caso não seja possível adotar de imediato as providências necessárias para a efetivação desses direitos, deve-se enviar resposta ao(à) titular indicando as razões que impediram a adoção imediata das providências.

Por outro lado, caso a instituição de ensino ou a secretaria não seja um(a) agente responsável pelo tratamento desses dados, essa resposta deverá, sempre que possível, indicar quem é o(a) agente responsável.

Além disso, quando os direitos de **correção, eliminação, anonimização ou bloqueio** forem atendidos, será necessário informar essas mudanças aos(às) agentes de tratamento com os(as) quais esses dados foram compartilhados para que os mesmos procedimentos possam ser repetidos. Isso apenas não será necessário nos casos em que esta comunicação for impossível ou implique esforço desproporcional.

IMPORTANTE

Antes de responder às solicitações dos(as) titulares, é preciso avaliar internamente se a solicitação de fato poderá ser atendida. Isso porque determinadas situações permitidas pela LGPD podem impedir que esses direitos sejam cumpridos (ex.: casos em que for solicitada a exclusão de um dado necessário para cumprimento de obrigações junto ao MEC).

OK

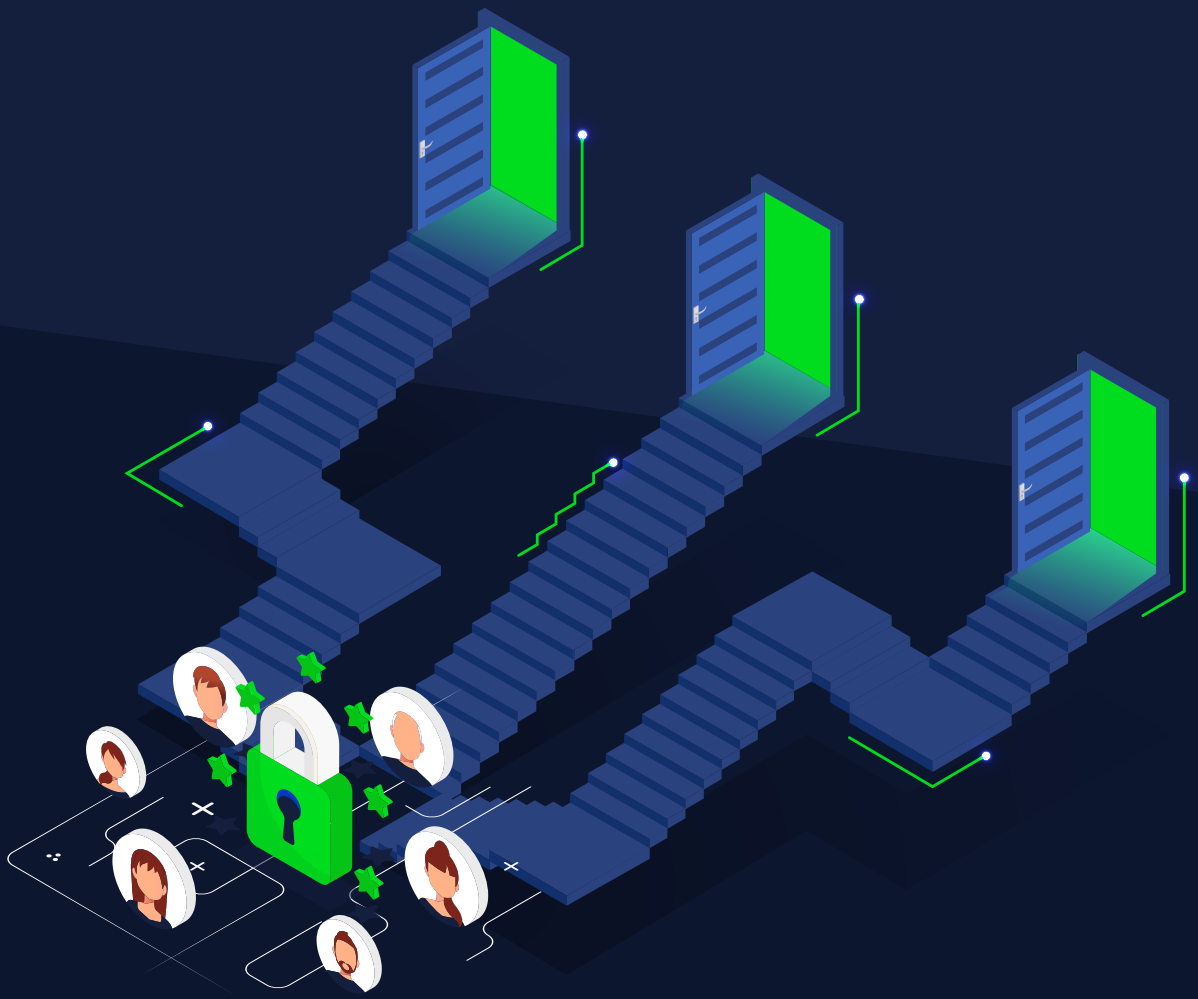
Qual o prazo para atender a esses direitos?

Direitos de confirmação de existência e o acesso aos dados pessoais: a resposta deve ser fornecida de modo imediato e em formato simplificado. Caso isso não seja possível, a resposta deve ocorrer por meio de declaração clara e completa, em até 15 dias da data do requerimento pelo(a) titular, a qual deve indicar origem dos dados, inexistência de registro, os critérios utilizados e a finalidade do tratamento, resguardados os segredos industrial e comercial.

Demais direitos: é recomendável que sejam atendidos de forma imediata. Contudo, prazos específicos para atender aos direitos dos(as) titulares podem vir a ser previstos pela ANPD (Autoridade Nacional de Proteção de Dados Pessoais).

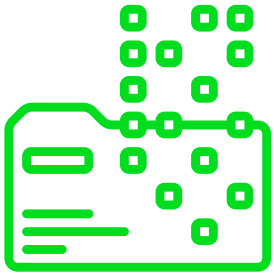
04.

CUIDADOS DURANTE AS ETAPAS DO CICLO DE VIDA DOS DADOS PESSOAIS



Agora que já conhecemos os principais conceitos da LGPD, vamos analisar os cuidados que devem ser adotados ao longo do ciclo de vida dos dados pessoais utilizados no ambiente educacional – ou seja, na coleta, uso, compartilhamento e armazenamento e eliminação dos dados.

01.



COLETA DE DADOS PESSOAIS

O que é?

Coleta de dados é a atividade de recebimento de um dado pessoal referente a um determinado indivíduo para utilizar esse dado no contexto das atividades da pessoa ou entidade que o coletou.

Para a prestação de serviços educacionais pelo poder público, as **secretarias de educação** (municipais e estaduais) costumam ser as principais responsáveis pela coleta de dados pessoais.[12]

A coleta de dados pessoais pode ser feita por meio de um documento **físico** (ex.: ficha cadastral enviada

[12] VALENTE, Patricia Pessôa; MICALI, Giovanna. LGPD e inovação no setor público: o caso das edutechs. in DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coord). LGPD e Administração Pública: uma análise ampla dos impactos. São Paulo: Revista dos Tribunais, 2020.

por escrito) ou por meio **digital** (ex.: quando o aluno ou a aluna realiza o seu cadastro em uma ferramenta educacional digital de terceiros oferecida pela escola). Além disso, a coleta de dados pessoais pode ocorrer de forma **direta**, quando a entidade recebe as informações diretamente do(a) titular dos dados (ex.: quando uma **secretaria de educação** recebe dados de estudantes para realização de matrícula ou quando disponibiliza formulário de solicitação de vaga *online*)[13] – ou **indireta**, quando existe um intermediário entre o(a) titular e a entidade que vai usar os seus dados (ex.: quando uma escola recebe as informações de estudantes por meio das secretarias de educação).

IMPORTANTE

Se a coleta de dados ocorrer de forma indireta, é recomendável firmar um acordo de transferência de dados pessoais, pelo qual as partes estabelecem direitos e obrigações relacionados ao uso desses dados. Esse acordo é considerado uma boa prática inclusive na transferência de dados entre secretarias de educação e escolas do ensino público.

OK

[13] Um exemplo prático disso é o formulário de pré-matrícula infantil disponível no site da Secretaria Municipal de Educação de São Paulo, no qual devem ser inseridas informações como: nome completo, sexo, país de origem, data de nascimento, raça, existência de deficiência e endereço da criança. Além disso, há também a coleta de dados dos responsáveis legais, preferencialmente os pais. Disponível em: https://cadastroinfantil.sme.prefeitura.sp.gov.br/. Acesso em: 06.08.2020.

O que fazer?

Como informado, a coleta de dados é uma atividade corriqueira no âmbito escolar e das secretarias de educação. Nesse contexto, um ponto muito importante está relacionado à **obrigação de informar ao(à) titular dos dados que os seus dados estão sendo coletados**. Isso pode ser feito, por exemplo, por meio de uma política de privacidade, em uma cláusula contratual, nos formulários de matrícula ou por meio de um *pop-up* específico em alguma tecnologia educacional ou site.

DICA

É possível dispor de políticas de privacidade aplicadas a mais de uma escola da rede de ensino, desde que as atividades de tratamento realizadas sejam similares. Essas políticas são um instrumento interessante para que organizações que usam dados cumpram com seus deveres de transparência. Isso porque, em apenas um documento, é possível informar todas as atividades de tratamento, as finalidades e os cuidados com dados pessoais da organização, além dos direitos dos titulares desses dados. [14]

OK

[14] Um exemplo de política de privacidade aplicada para escolas públicas pode ser observado por meio de de exemplos estrangeiros, como o do Agrupamento de Escolas Dr. Serafim Leite (Disponível em: http://essl.pt/images/Modulos_pag_principal/RGPD_AESL_signed.pdf) e da Escola Secundária João Gonçalves Zarco (Disponível em: https://www.zarco.pt/site/index.php/polprivacidade/), ambas de Portugal. Em âmbito nacional, um exemplo é a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual de Pernambuco, Decreto Estadual nº 49.265, de 6 de agosto de 2020 (Disponível em: https://legis.policiacivil.pe.gov.br/L2/resources/docs/3dca01e3b7c6c033c39d11fd7b3019aa.pdf), que institui a Política de Proteção de Dados Pessoais em consonância com a LGPD.

Além do dever de informar, alguns cuidados adicionais devem ser tomados.

Quando não preciso do consentimento para coletar dados pessoais?

Em geral, quando os dados pessoais estão sendo coletados para **finalidades relacionadas à educação e ao cumprimento de políticas públicas**, o consentimento não será necessário para a coleta dos dados. Isso porque o consentimento é apenas uma das formas de justificar a coleta de dados pessoais, sendo que existem diversas outras formas de realizar essa coleta de forma legítima.

Assim, algumas das situações mais comuns que justificariam o tratamento de dados no setor educacional são: (i) obrigação legal ou regulatória; (ii) execução de políticas públicas por órgãos públicos; (iii) execução de contratos ou procedimentos preliminares a esse, desde que o(a) titular dos dados seja parte desses contratos/procedimentos; (iv) quando se tratar de uso legítimo para que o órgão possa cumprir suas finalidades; dentre outras. O tópico **"Quando posso tratar dados pessoais"** apresenta informações mais detalhadas sobre essas finalidades.

SAIBA MAIS

ATENÇÃO ☒

De acordo com a LGPD, os dados pessoais de crianças que dependem de consentimento para serem tratados somente poderão ser coletados sem o consentimento parental quando a coleta for necessária justamente para contatar os familiares ou responsáveis legais: desde que esses dados sejam utilizados uma única vez e sem armazenamento, ou então para a proteção da criança, sendo que, em nenhuma hipótese, poderão ser repassados a terceiros sem o devido consentimento. Essa hipótese dialoga inclusive com o ECA, que considera dever da família, da comunidade, da sociedade em geral e do poder público assegurar com prioridade a efetivação dos direitos das crianças e adolescentes referentes a questões como a vida e a saúde (ex.: primazia de receber proteção e socorro em quaisquer circunstância).

OK

Quando preciso do consentimento para coletar dados pessoais?

O consentimento será necessário normalmente quando a secretaria ou escola querem usar os dados para uma finalidade fora do contexto educacional ou quando envolver uso de fotos, vídeos e biometria de estudantes, familiares, servidores e servidoras públicas.

Exemplo 1: Será necessário obter o consentimento caso se esteja coletando fotos e vídeos de estudantes para publicá-los em material de publicidade institucional.

Exemplo 2: Outro exemplo ocorre nos casos em que, para utilizar funcionalidades de uma plataforma educacional *online*, o aluno ou a aluna deve fornecer o seu consentimento (como no caso específico que autoriza a plataforma a acessar a câmera, capturar imagens e vídeo do dispositivo utilizado ou acessar dados de localização).

IMPORTANTE

No caso de coleta indireta, o consentimento será necessário não apenas para a coleta do dado, mas também para o seu compartilhamento com outras pessoas ou entidades.

OK

Como devo obter o consentimento?

Em geral, o consentimento deve ser obtido **no momento da coleta** dos dados. Isso pode ser feito de diversas maneiras, como por meio de cláusulas contratuais ou termos de consentimento. Também é possível que sejam utilizados instrumentos ainda mais específicos – dentre os quais se destacam os termos de cessão de uso de imagem ou voz.

Lembre-se de que o essencial é garantir que o consentimento seja obtido de maneira **livre, informada e inequívoca**. Nesse sentido, por exemplo, não seria possível afirmar que o(a) titular de dados consentiu adequadamente por meio de uma caixa pré-marcada na qual se afirma *"Dou consentimento para os tratamentos informados"*. Deve haver destaque para a obtenção do consentimento de maneira que fique claro ao(à) titular quais dados estão sendo coletados e para quais finalidades.

Lembre-se também de que, se os dados coletados pertencerem a **menores de 12 anos**, será necessário coletar o consentimento de seus familiares ou representantes legais (embora alguns argumentem que o consentimento parental seja aplicável aos menores de 16 anos).

ATENÇÃO ☒

Recomendamos que a parte responsável (entidade do sistema de educação ou terceiros) por coletar o consentimento dos familiares e responsáveis seja capaz de demonstrar que adotou esforços razoáveis para obtê-lo de de forma válida, adotando mecanismos antifraude.

OK

OBSERVAÇÃO ☒

No geral, as próprias ferramentas tecnológicas que tratam dados de estudantes e docentes terão condições de pedir o consentimento dos(das) titulares para que possam usar suas funcionalidades. Esse consentimento pode ser aproveitado pela própria escola ou secretaria, que não precisará obter outro consentimento do(a) titular. Entretanto, em algumas situações, a depender de quem possui contato direto com o(a) titular de dados ou seus representantes legais, pode ser que a própria escola ou secretaria tenha que obter o consentimento para aplicar a tecnologia.

OK

O que mais eu devo saber sobre a coleta?

É importante verificar a autenticidade dos dados coletados. Isto é, verificar se eles estão corretos. Para isso, é recomendável avaliar a fonte dos dados – especialmente em caso de coleta indireta. Isso se deve ao fato de que o uso de dados incorretos pode gerar impactos negativos para seus/suas titulares.

Além disso, nos casos em que os(as) titulares dos dados forem **crianças e adolescentes**, a sua coleta também deverá levar em conta critérios que busquem proteger esse público, conforme disposto no ECA, como através da preservação da imagem, da identidade, da autonomia e das crenças desses indivíduos.

Como fazer?

A LGPD determina que o consentimento significa uma **manifestação livre, informada e inequívoca**, pela qual o(a) titular concorda com o uso dos seus dados pessoais para uma finalidade determinada.

Para que o consentimento seja **livre**, é preciso que esse consentimento seja uma escolha genuína do(a) titular. Em outras palavras, a existência de elementos que influenciem ou pressionem o(a) titular de maneira inapropriada e que o(a) impeçam de exercer o seu livre arbítrio podem tornar esse consentimento inválido.

Exemplo: A solicitação de consentimento para tratamento de dados pessoais no contexto de relações de trabalho entre a secretaria e o funcionalismo público não costuma ser a base legal mais adequada, especialmente pela assimetria de poder entre as partes.

Para que o consentimento seja **informado**, é recomendável que informações como as seguintes sejam transmitidas ao(à) titular:

1. quem é o controlador ou a controladora dos dados pessoais,
2. qual a finalidade para o tratamento dos dados,
3. quais os tipos de dados utilizados e
4. existência da possibilidade de revogação desse consentimento.

Além disso, é importante que essas informações sejam passadas de maneira clara, acessível e de fácil leitura, sendo inclusive adequada ao seu público-alvo. Essa prestação de informações geralmente é realizada na política de privacidade, em instrumentos contratuais e/ou em outras interfaces com o(a) titular de dados.

Exemplo 1: Caso o tratamento de dados seja endereçado a menores de idade, é recomendável que a solicitação de consentimento seja apresentada em linguagem adequada ao público infantil.

Exemplo 2: Caso o consentimento seja informado por escrito, a informação sobre a solicitação do consentimento deverá constar de cláusula destacada das demais cláusulas contratuais.

A LGPD também não impede que o consentimento seja obtido de **forma oral**. Para tanto, as informações fornecidas ao(à) titular devem ser claras e inteligíveis, e o controlador ou a controladora deve solicitar uma confirmação específica pelo(a) titular a fim de comprovar o consentimento fornecido.

Exemplo 1: Caso o consentimento seja coletado por meio de contato telefônico, deve-se solicitar que o(a) titular aperte um determinado botão ou forneça oralmente uma resposta afirmativa, como: *"Permaneça na linha e responda 'sim' ou então aperte a tecla '1' caso concorde com o tratamento de seus dados pessoais para as seguintes finalidades: [atendente deve descrever finalidades].".*

Quando o consentimento for necessário para o tratamento de **dados pessoais sensíveis**, a coleta desse consentimento deve ocorrer de forma **específica** e **destacada**. Isso significa que é necessária uma declaração afirmativa de que esse consentimento foi coletado.

Exemplo: O consentimento para dados pessoais sensíveis pode ser solicitado através de *opt-in* em caixa de verificação ou assinatura escrita ou eletrônica, em apartado da solicitação do consentimento para outras finalidades.

02.

USO DOS DADOS PESSOAIS

O que é?

O uso de dados se refere a qualquer atividade que tenha como base os dados pessoais coletados.

Os exemplos de uso de dados para fins de educação são os mais variados possíveis. Com a inserção de ferramentas tecnológicas na educação, foram

criadas inúmeras formas de gerar informação e usar dados para ajudar no desempenho pedagógico de estudantes, na formação de docentes e na gestão educacional de escolas, por exemplo.

Atualmente, existem ferramentas que geram automaticamente relatórios sobre o engajamento e o desempenho dos(as) estudantes nas avaliações, além de produzir portfólios individuais e personalizados, com o mapeamento de todas as interações nos cadernos.

Além disso, existem tecnologias que usam inteligência artificial para registrar as atividades dos(as) estudantes enquanto interagem com os recursos oferecidos (leituras, revisões, exercícios e outros) e, assim, gerar gráficos de desempenho em tempo real.

Todas essas ferramentas envolvem inúmeros dados pessoais de estudantes e docentes e podem ser valiosas para os processos de ensino-aprendizagem e para auxiliar gestores e gestoras educacionais em suas funções. Mas alguns cuidados são necessários no uso desses dados, conforme veremos a seguir.

O que fazer?

Em linhas gerais, os cuidados que devem ser tomados em qualquer uso de dados pessoais são:

- Sempre informar ao(à) titular dos dados que você está usando seus dados pessoais e a finalidade disso (seja por meio de política de privacidade, de contrato ou outras interfaces disponíveis);
- Sempre que possível, evitar usar dados pessoais como raça/cor, gênero, renda, orientação sexual, que possam levar a algum tipo de discriminação;
- Somente usar aqueles dados pessoais necessários e imprescindíveis para cumprir a finalidade pretendida; e
- Restringir o acesso aos dados pessoais às pessoas que efetivamente precisam dessas informações para desenvolver suas funções (por meio, por exemplo, da adoção de uma política de controle de acessos dentro da instituição).

As quatro situações acima representam recomendações gerais que devem permear qualquer uso de dados pessoais no âmbito da gestão pública educacional.

Em algumas **situações específicas**, no entanto, é necessário ter cuidados adicionais no uso dos dados pessoais. A seguir, exemplificamos essas situações.

Criação de perfis

O que é?

A criação de perfis é o processo de usar dados de um determinado indivíduo para criar padrões e tomar decisões em cima dos padrões criados. Isso pode ser feito **tanto por humanos como por máquinas**.

Exemplo: Diversas ferramentas educacionais digitais têm como funcionalidade traçar perfis de estudantes e docentes para entender melhor alguns dos seus comportamentos (como desempenho e assiduidade acadêmicos) e auxiliar a gestão e a equipe de educação no acompanhamento pedagógico. Esses perfis, por sua vez, podem ser criados tanto a partir de decisões automatizadas, isto é, por algoritmos e outros atributos técnicos da ferramenta, quanto por humanos.

O que fazer?

Em primeiro lugar, é muito importante informar ao indivíduo que seu perfil está sendo criado. Isso deve estar previsto na política de privacidade da ferramenta usada.

Além disso, o gestor e a gestora educacional devem verificar se, para a criação dos perfis,

os dados não estão sendo utilizados de forma a gerar discriminação, com especial cuidado com dados de raça/cor, gênero, renda, saúde.

OBSERVAÇÃO

É possível que dados como raça/cor e renda sejam utilizados para pensar em políticas públicas específicas a partir dessas informações. De todo modo, é recomendável evitar o uso desses dados para gerar perfis de acompanhamento pedagógico, justamente devido aos riscos que podem acarretar para os(as) titulares.

OK

Decisões automatizadas

O que é?

Decisões baseadas em tratamento automatizado de dados pessoais ocorrem quando alguma das etapas do tratamento de dados é realizado por uma máquina ou algoritmo. Isso ocorre, por exemplo, em ferramentas que usam inteligência artificial para corrigir redações de estudantes.

Além disso, decisões automatizadas são muito comuns nos casos de definição de perfis de estudantes ou profissionais do serviço público.

O que fazer?

Assim como no caso mencionado acima, é necessário informar ao(à) titular dos dados que é realizado tratamento automatizado de seus dados.

Além disso, quando o tratamento dos dados ocorrer de forma automatizada, é necessário garantir ao(à) titular o direito de revisão de decisões tomadas que possam afetar os seus interesses, além de permitir que entendam quais foram os critérios utilizados para o alcance da decisão automatizada.

Envio de comunicações para os(as) titulares de dados

O que é?

É comum, no ambiente educacional, a comunicação com titulares dos dados para passar informações sobre atividades escolares, seja diretamente para o(a) titular dos dados ou para seus responsáveis.

Atualmente, existem ferramentas que facilitam a comunicação em ambientes de chat de docentes com estudantes e docentes com responsáveis legais, além de mecanismos de mensagens automáticas para

familiares e responsáveis para avisar quando o aluno ou a aluna falta da escola. No geral, essas comunicações estão dentro do escopo educacional, mas alguns cuidados devem ser tomados no uso de tecnologias específicas para essas funcionalidades.

O que fazer?

É importante verificar se essas comunicações se resumem às finalidades institucionais ou se as ferramentas podem usar os contatos de familiares, estudantes e docentes para outras finalidades, como oferecer produtos por meio de marketing direto.

Caso a ferramenta utilize dados dos contatos para oferta de produtos, é importante se certificar de que essa ferramenta pede o consentimento dos(as) titulares para essas atividades. Esse consentimento normalmente é obtido por meio de *opt-in* – isto é, uma caixa de seleção em que a pessoa clica para indicar que aceitar receber comunicações com ofertas de produtos e serviços.

Como gestor ou gestora, o importante é verificar se a ferramenta está obtendo o consentimento para essas comunicações, se esse consentimento está sendo obtido da forma correta, e orientar educadores e educadoras sobre os cuidados que devem ser tomados no uso dessas ferramentas no ambiente escolar.

Uso de foto, imagem e voz

O que é?

Tradicionalmente, no ambiente educacional, fotos e imagens são usadas para diversos fins, como para controle de identidade, segurança e para a realização de atividades educacionais (ex.: publicação de fotos de estudantes em mural da escola, publicação em portfólio, etc).

Entretanto, com a inserção de tecnologias no meio educacional, imagens e fotos de estudantes passaram a ser utilizadas para outras funcionalidades, como controle de presença a partir de biometria, realização de atividades com vídeos gravados de estudantes, entre outras. Essas situações exigem alguns cuidados adicionais por parte da gestão.

O que fazer?

Normalmente, a própria ferramenta exigirá o consentimento das pessoas para que possa gravar fotos e vídeos durante o seu funcionamento. A princípio, esse consentimento é suficiente para cumprir a LGPD. Em algumas situações, no entanto, a depender de como são usadas as imagens, é recomendável que gestores e gestoras educacionais orientem as escolas para que coletem diretamente o consentimento dos(as) estudantes e dos familiares para o uso da imagem ou voz.

Além disso, é importante que os(as) titulares dos dados, ao acessarem uma política de privacidade referente a uma determinada tecnologia, sejam informados sobre as atividades de tratamento realizadas por essa tecnologia que envolvem uso de imagens, vídeos e voz (ex.: através de um *pop-up* específico para informar essas atividades).

Tal qual indicado acima, é recomendável que gestores e gestoras verifiquem se a ferramenta está obtendo o consentimento para esse uso dos dados, se esse consentimento está sendo obtido da forma correta, e orientar educadores e educadoras sobre os cuidados que devem ser tomados no uso dessas ferramentas no ambiente escolar.

Uso de dados de saúde

O que é?

É comum que dados de saúde sejam usados tanto para proteção quanto para monitoramento de estudantes e docentes no ambiente escolar. No entanto, seu uso vem sendo expandido, inclusive para algumas ferramentas tecnológicas direcionadas à saúde em ambiente escolar.

Devemos lembrar que dados de saúde são **dados pessoais sensíveis**, portanto, é importante observar com mais cautela as ferramentas que usam essas informações.

Exemplo: Ferramentas que permitem a interação entre familiares, estudantes e docentes e fornecem informações sobre alimentação, saúde e higiene durante o período escolar.

No âmbito da gestão escolar, existem tecnologias que auxiliam no gerenciamento de fichas médicas e outros recursos. Essas ferramentas podem armazenar e usar dados de saúde de estudantes e docentes para outras finalidades.

O que fazer?

No uso de dados de saúde a partir de ferramentas tecnológicas, é recomendável também coletar o consentimento das pessoas.

Nesse casos, o consentimento deve ser obtido de forma destacada para a finalidade específica que requer a sua coleta.

Recomenda-se, mais uma vez, que verifiquem se a ferramenta está obtendo o consentimento para o uso de dados de saúde, se esse consentimento está sendo obtido da forma correta, e orientem educadores e educadoras sobre os cuidados que devem ser tomados no uso dessas ferramentas no ambiente escolar.

03.

COMPARTILHAMENTO DE DADOS PESSOAIS

O que é?

O compartilhamento de dados pessoais engloba uma série de atividades, como a comunicação de dados, a sua difusão, ou o tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas ou entre estes e entes privados.

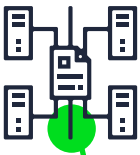
Na gestão educacional, dados pessoais podem ser compartilhados por diversas finalidades, como para a gestão de políticas educacionais entre órgãos e entidades públicas, transferência de dados entre secretarias de educação e escolas para prestação de serviços públicos, entre outras finalidades.

O compartilhamento também pode ocorrer com organizações privadas que sejam fornecedoras ou prestadoras de serviços, bem como durante o uso de recursos educacionais digitais. Nesse último caso, os dados gerados no uso de ferramentas tecnológicas podem ser utilizados tanto pelo órgão público que contratou quanto pela empresa fornecedora da tecnologia.

Os termos de compartilhamento podem ser definidos por meio de obrigações legais ou regulatórias, ou firmados com base em contrato.

O uso posterior dos dados compartilhados, inclusive, pode estar sujeito a finalidades predeterminadas (quando é estabelecido como o receptor dos dados deve usá-los), a depender das condições de compartilhamento, ou não – ficando o receptor dos dados mais livre para os utilizar para suas próprias finalidades.

Na gestão educacional, um dos primeiros passos para o compartilhamento de dados pessoais é a definição do porquê. Ou seja, é necessário haver uma finalidade para o compartilhamento, que pode ser uma obrigação legal, a execução de políticas públicas, a prestação de um serviço público, ou até mesmo um contrato ou parceria com entidades públicas e privadas.



O que fazer?

É importante informar ao(à) titular dos dados que os seus dados pessoais podem ser compartilhados com terceiros, com quais terceiros esses dados podem ser compartilhados, e qual é a finalidade do compartilhamento.

DICA

Como já mencionado anteriormente, informações sobre o compartilhamento de dados pessoais podem estar dispostas em política de privacidade.

OK

Como compartilhar dados?

É importante que os termos do compartilhamento estejam previstos e descritos em um contrato entre o detentor ou a detentora dos dados e o receptor ou a receptora.

Tais instrumentos jurídicos permitem maior segurança às partes e aos(às) titulares dos dados que serão compartilhados. A partir de cláusulas contratuais, é possível delimitar e estabelecer diretrizes para os usos posteriores dos dados pessoais sujeitos ao compartilhamento. Um cuidado importante, nesse sentido, é garantir que o receptor ou receptora dos dados se obrigue a cumprir com o disposto na LGPD, reafirmando a importância da proteção de dados. Além disso, é essencial que os dados compartilhados atendam a propósitos lícitos e legítimos, ou seja, que eles possam ser utilizados na medida em que se deseja.

Preciso coletar consentimento para compartilhar dados?

Normalmente, o consentimento para compartilhar dados pessoais será necessário se o dado foi originalmente coletado mediante consentimento.

Exemplo: Uma escola aplica uma ferramenta em sala de aula que grava imagens dos(as) estudantes. Essa ferramenta exige o consentimento para coletar essas imagens. A escola posteriormente deseja compartilhar essas imagens com algum terceiro. Nesse caso, será necessário obter o consentimento para realizar o compartilhamento, uma vez que o dado pessoal (imagem) foi originalmente coletado por meio do consentimento.

Com quem posso compartilhar dados pessoais?

O compartilhamento pode ser realizado tanto com órgãos e entidades públicas quanto com organizações privadas. Na prática, as possibilidades, regras e recomendações no compartilhamento irão variar caso o receptor seja privado (ex.: empresa de marketing, empresa de processamento de dados, dentre outros) ou público (ex.: escola municipal ou estadual, secretaria de educação municipal ou estadual, dentre outros). Por conta disso, serão analisadas abaixo as especificidades em relação a esses receptores.

Como compartilhar dados com órgãos públicos?

O compartilhamento de dados com órgãos públicos deve ser realizado em função do interesse público, podendo decorrer de obrigação legal ou para execução de políticas públicas.

No caso de obrigação legal (ex.: compartilhamento com o MEC para a realização do Censo Escolar), gestores e gestoras devem verificar quais dados são exigidos pela legislação aplicável, não devendo ser compartilhados dados não solicitados legalmente. Isso porque não haveria justificativa para compartilhar dados adicionais não requeridos em lei. Atente-se aqui aos já mencionados princípios da finalidade, necessidade e adequação, que poderiam ser feridos em caso de compartilhamento excessivo de dados.

Já no caso de execução de políticas públicas, cabe à gestão analisar adequadamente os dados que são estritamente necessários para que as atividades sejam realizadas.

Vale também mencionar que, quando possível, os dados deverão ser mantidos em formatos interoperáveis para a execução de políticas públicas e utilização por outros órgãos públicos.

Algumas perguntas podem ajudar a orientar o compartilhamento de dados pela gestão:

Preciso receber ou enviar todos esses dados pessoais para executar a política pública?

Existem dados que não precisam ser compartilhados para cumprir a finalidade pretendida?

A depender da resposta, pode-se optar por reduzir ou limitar os dados compartilhados e até mesmo utilizar dados anonimizados – caso esses sejam suficientes para cumprir os objetivos da política pública em questão.

Em ambas as possibilidades, é necessário que os órgãos públicos que compartilham os dados forneçam informações aos(às) titulares sobre quais dados são compartilhados, com quem e para quais finalidades. Atente-se que esses pontos são importantes para garantir plenamente os direitos dos(as) titulares de dados já mencionados neste manual.

Como compartilhar dados com particulares?

O compartilhamento de dados com particulares deverá sempre almejar o alcance do interesse público, devendo sempre ser justificável na perspectiva da proteção de dados. Isso significa que deve haver uma justificativa lícita e legítima para o compartilhamento. No caso do setor educacional, esse compartilhamento com entes privados pode ocorrer preferencialmente:

1. para execução de políticas públicas; ou

2. com o consentimento dos titulares.

Os contratos já mencionados assumem particular relevância no caso de compartilhamento com particulares para fins de definição de parâmetros para o uso dos dados pelo receptor ou receptora. Assim, é recomendável que sejam inseridas cláusulas de proteção de dados nos contratos administrativos com os particulares, e que sejam compartilhadas apenas informações estritamente necessárias para o cumprimento dos objetivos propostos.

Compartilhamento de dados no uso de recursos educacionais digitais

É comum que os dados gerados no uso de recursos tecnológicos sejam compartilhados entre a empresa fornecedora da ferramenta e o órgão público que contratou sua aplicação.

Nesses casos, é importante estabelecer em contrato as condições e requisitos para o uso desses dados pelo desenvolvedor da ferramenta (ver mais no tópico **“Cuidados na Contratação de Recursos Educacionais Digitais”**).

SAIBA MAIS

04.

PUBLICAÇÃO DE DADOS PESSOAIS

O que é?

A publicação de dados pode tanto ocorrer devido a um dever de publicidade e transparência em obrigações de órgãos públicos por força de lei, principalmente quando se observa o disposto na Lei nº 12.527/2011 (“Lei de Acesso à Informação” ou “LAI”), como por decisão da gestão.

Dever de publicidade e transparência

A Constituição Federal apresenta como um dos direitos fundamentais dos cidadãos e das cidadãs receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, com exceção daquelas informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Para tanto, a publicação da LAI visa garantir o acesso a informações previsto na Constituição, ao nortear a efetivação desse direito.

O princípio da publicidade, nesse sentido, assegura a ampla divulgação dos atos de pessoas jurídicas

submetidas ao regime jurídico de direito público. A LAI, portanto, determina a obrigação de fornecer informações de interesse público, independente de solicitação (transparência ativa), ou após demanda apresentada por cidadão(ã) (transparência passiva).

Isso implica afirmar que, em algumas situações, o interesse público se sobrepõe à privacidade individual, sustentando a possibilidade de publicação, referendada, inclusive, em entendimentos do STF.

É recomendável, ademais, que, mesmo em caso de publicação de dados em razão de obrigação legal, sejam tomadas medidas ou implementados mecanismos tecnológicos que mitiguem os riscos à privacidade daqueles que têm seus dados publicados, de modo a garantir o cumprimento da LAI com a menor interferência possível a direitos fundamentais.[15-16]

Exemplo: Publicação de dados de servidoras e servidores públicos quando necessário para atendimento do princípio da publicidade administrativa.

Ressalta-se, por fim, que as obrigações da LAI devem ser sempre compatibilizadas com a própria LGPD. Nesse sentido, a LAI e a LGPD devem ser vistas a

[15] STF, Agravo Regimental na Suspensão de Segurança no. 3.902/SP, Rel. Min. Ayres Britto, j. 3/10/2011.

[16] Nesse sentido, manifestou-se o STF também na Suspensão de Segurança no. 3.902/SP: "Não cabe, no caso, falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo "nessa qualidade" (§6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados

partir de um viés de complementaridade. Mesmo que os dados sejam publicados por obrigação legal, tornando-se acessíveis publicamente, é necessário considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização - caso se deseje realizar quaisquer atividades de tratamento com base nesses mesmos dados.

Vale ressaltar, contudo, que a LGPD não incompatibiliza o cumprimento da LAI. Pelo contrário: a própria LGPD, embora possua uma maior abrangência, determina expressamente que a sua aplicação não dispensa os órgãos públicos de cumprir as determinações de que trata a LAI.

Decisão da gestão

Além disso, a publicação pode ocorrer em âmbito geral, para quaisquer interessados, ou em âmbito restrito, como apenas a estudantes de determinada escola (ex.: divulgação das frequências escolares em listas dispostas nas áreas de circulação do local).

Em ambos os casos, e em conformidade com o que foi dito acerca do compartilhamento, as hipóteses de publicação devem ser justificáveis de acordo com os princípios e direitos da LGPD e de acordo com as hipóteses de tratamento de dados pessoais – correspondendo a determinado interesse público que

em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. A negativa de prevalência do princípio da publicidade administrativa implicaria, no caso, inadmissível situação de grave lesão à ordem pública". STF, Agravo Regimental na Suspensão de Segurança no. 3.902/SP, Rel. Min. Ayres Britto, j. 3/10/2011.

seja relevante o suficiente para justificar a publicização das informações mencionadas.

O que fazer?

Informar os(às) titulares sobre as possibilidades em que seus dados poderão ser publicados.

Exemplo: Informar em política de privacidade que dados como o de alunos e alunas aprovadas em processos seletivos e listas de presenças poderão ser divulgados publicamente.

Por que estou publicando dados?

É importante notar que deve haver uma justificativa para a publicação dos dados pessoais. Isso porque, caso não haja um interesse público suficientemente relevante, é possível que a divulgação de dados pessoais seja considerada como excessivamente intrusiva à privacidade dos(as) titulares de dados, além de implicar no risco de uso indevido desses dados.

No geral, dados pessoais poderão ser publicados em decorrência de obrigação legal, política de dados abertos, em pedidos de acesso à informação, como nos casos dispostos na LAI, ou por decisão própria da gestão.

Como publicar dados em caso de políticas de transparência e dados abertos?

Informações geradas no ambiente da educação pública básica estão submetidas a políticas de transparência e dados abertos, como ressaltado, em decorrência de obrigações dos órgãos públicos. No caso de informações pessoais, é necessário ponderar os benefícios e riscos na divulgação – considerando também o dever essencial em torno da transparência. Sempre que possível, deve-se optar pela divulgação de dados de maneira anonimizada.

Assim, caso os dados sejam divulgados, será necessário adotar cuidados, tais como a restrição de uso e/ou a imposição de salvaguardas técnicas. Atente-se que a restrição de uso, por exemplo, é essencial para o cumprimento dos princípios em matéria de proteção de dados – finalidade, necessidade e adequação.

Ademais, é possível que, em determinados casos, a publicação seja padronizada a fim de atender os objetivos da LAI, por meio do uso de portais oficiais governamentais e outros mecanismos - demandando a conformidade com normas aplicáveis a nível estadual ou municipal.

Exemplo 1: Um exemplo de divulgação de dados pessoais por força de lei se refere à divulgação do nome e salário de docentes contratados pelo governo federal. Isso ocorre por conta da obrigação de transparência atrelada aos servidores e às servidoras públicas, na medida em que eles são remunerados por meio de recursos da administração pública.[17]

Exemplo 2: Outro exemplo é o caso do aplicativo Clique Escola, do MEC, cujo objetivo é dar transparência a informações educacionais e a dados financeiros de mais de 180 mil escolas públicas e privadas de educação básica no familiares. A plataforma traz informações como nota de cada escola no Sistema de Avaliação da Educação Básica (Saeb) por ano, etapa de ensino e disciplina; distorção idade-série por ano e etapa de ensino; média de estudantes por turma e por etapa de ensino; porcentagem de docentes com curso superior por ano e etapa de ensino; taxas de rendimento, aprovação, reprovação e abandono, por etapa de ensino. As informações são extraídas das bases de dados do Fundo Nacional de Desenvolvimento da Educação (FNDE) e do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep).[18]

[17] Nos termos do Recurso Extraordinário com Agravo no. 652777/SP: "Caso em que a situação específica dos servidores públicos é regida pela 1ª parte do inciso XXXIII do art. 5º da Constituição. Sua remuneração bruta, cargos e funções por eles titularizados, órgãos de sua formal lotação, tudo é constitutivo de informação de interesse coletivo ou geral. Expondo-se, portanto, a divulgação oficial. Sem que a intimidade deles, vida privada e segurança pessoal e familiar se encaixem nas exceções de que trata a parte derradeira do mesmo dispositivo constitucional (inciso XXXIII do art. 5º), pois o fato é que não estão em jogo nem a segurança do Estado nem

Quando eu posso publicar dados pessoais de estudantes?

Nesse caso, trata-se de publicação por decisão da gestão, portanto, deve-se atentar às recomendações dadas acima. Essa publicação, por sua vez, pode ser realizada de forma a abarcar, de modo mais ou menos limitado, diversos públicos – apenas estudantes de determinada escola, familiares e docentes, público em geral, dentre outras possibilidades.

Sempre que forem publicados dados pessoais de estudantes, é necessário, como destacado, avaliar os benefícios da divulgação e os efeitos disso aos(às) titulares de dados.

do conjunto da sociedade". Recurso Extraordinário com Agravo no. 652777/SP, Rel. Min. Teori Zavascki, j. 23.04.2015.

[18] Ministério da Educação. "MEC lança aplicativo para dar transparência a dados educacionais e financeiros de escolas". Disponível em: http://portal.mec.gov.br/component/content/article?id=86531. Acesso em: 31.08.2020.

Exemplo 1: a divulgação de notas de estudantes de maneira aberta em site de determinada escola para quaisquer interessados. Nesse caso, recomenda-se que a divulgação das notas não possa ser acessada por qualquer pessoa, dado que tal possibilidade seria excessivamente intrusiva à privacidade e não traria benefícios gerais que sustentassem o atendimento do interesse público. Por esse motivo, quando notas forem publicadas, o ideal é que sejam acessíveis apenas por meio de *login* e senha por estudantes e seus responsáveis legais. [19-20]

Exemplo 2: o uso de listas em vias físicas ou em meios *online* para a divulgação da separação dos(as) estudantes em relação a classes, docentes e ano escolar. Nessa situação, caso seja disponibilizada lista física, é recomendável que esta seja disposta em locais de fácil acesso aos(às) estudantes e aos responsáveis legais por tempo razoável para que tomem conhecimento das informações. Além disso, caso ocorra a disponibilização em meio *online*, como site de determinada escola, o ideal é que as informações sejam dispostas individualmente por meio de *login* e senha.[21]

[19] Garante Privacy. "Autoridade italiana publica esclarecimentos sobre publicação de notas em contexto escolar". Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9367295. Acesso em: 22.07.2020.

[20] A agência espanhola de proteção de dados (AEPD) produziu um guia de proteção de dados para escolas, com base na legislação de proteção de dados da União Europeia, com informações e orientações que podem servir de referência para redes de ensino brasileiras. Agencia Española

O que fazer em relação ao consentimento?

É importante destacar que os dados coletados com consentimento dificilmente poderão ser tornados públicos – a menos que o(a) titular tenha consentido especificamente para essa finalidade. Assim, caso se deseje divulgar os dados mencionados, de modo geral, será necessário obter o consentimento posterior e específico para tal ação.

De toda forma, é recomendável que dados pessoais sensíveis não sejam divulgados, considerando sua natureza extremamente íntima e privada (ex.: dificilmente seria possível justificar a divulgação de informações a respeito da saúde dos(as) estudantes em determinada escola).

de Protección de Datos (AEPD). "Guía para Centros Educativos". p. 28. Disponível em: http://tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf. Acesso em: 23.07.2020.

[21] Agencia Española de Protección de Datos (AEPD). "Guía para Centros Educativos". p. 29. Disponível em: http://tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf. Acesso em: 23.07.2020.

05.

ARMAZENAMENTO E EXCLUSÃO DE DADOS

O que é?

Armazenamento

O armazenamento de dados pessoais envolve qualquer **ação ou resultado da manutenção ou conservação** desses dados pessoais.[22]

O armazenamento de dados pessoais pode ser feito de maneira **física ou digital**, sendo que a LGPD se aplica a ambos os casos. Isso significa que, mesmo que os dados pessoais estejam armazenados em meios físicos, os preceitos de proteção de dados deverão ser observados (ex.: arquivos físicos que preservam informações sobre estudantes em ordem alfabética, por ano escolar ou a partir de outros critérios). Já quando se trata de meios digitais, os dados podem ser armazenados a partir de servidores locais ou em nuvem. Em ambos os casos, esses servidores podem ser locais ou estar situados no exterior.

[22] Governo Federal. "Guia de Boas Práticas para Implementação na Administração Pública Federal", p. 9. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 21.08.2020.

Atente-se para o fato de que, no caso de estarem localizados fora do país (como no caso de armazenamento de dados pessoais em servidores em nuvem), existem leis específicas que podem ser aplicadas para regular esse armazenamento (normas locais desse outro país). Por conta disso, é importante levar em consideração esses fatores no momento de escolher a forma que será utilizada para o armazenamento dos dados pessoais envolvidos no setor educacional.

O armazenamento, inclusive, não se refere apenas aos dados pessoais de estudantes, mas sim a todos aqueles que sejam, de alguma maneira, armazenados no setor educacional, abarcando docentes, profissionais, dentre outros.

Exclusão

Os dados pessoais só podem ser mantidos caso haja motivos para isso. Como consequência, quando esse armazenamento não puder ser justificado, há um forte indicativo de que os dados devem ser excluídos. Portanto, a exclusão dos dados pessoais é uma etapa obrigatória e relevante quando as finalidades de armazenamento se esgotaram.

A questão da exclusão será conjuntamente tratada com o armazenamento, considerando as conexões entre as matérias quando se fala em proteção de dados.

O que fazer?

Em primeiro lugar, é importante verificar onde são armazenados os dados sob guarda da secretaria ou escola (servidores locais, nuvem, arquivos físicos).

Dados armazenados em servidores locais

No armazenamento em servidores locais, é importante verificar o tempo de armazenamento, o nível de segurança empregado e o controle de acesso a esses dados – os quais devem ser especialmente observados na medida em que a escola ou secretaria estará diretamente na posição de avaliar o tratamento dos dados. Isso porque, quando se contrata uma empresa fornecedora de armazenamento em nuvem, por exemplo, pode-se não ter acesso direto a todas as etapas, sendo a maior transparência uma possível vantagem dos servidores locais. Nessa situação, então, não há que se preocupar com a questão da transferência internacional de dados. Porém, a estrutura de armazenamento deve ser passível de responder, em tempo adequado, às demandas dos(as) titulares de dados – se estas ocorrerem.

Em relação ao tempo de armazenamento, valem as mesmas regras gerais para outras formas de armazenar dados. Assim, é importante avaliar por quanto tempo os dados serão armazenados, traçando políticas internas ou observando normas ou leis específicas que indiquem prazos a depender do tipo de dado e do

ente. Nesse sentido, é relevante que os dados sejam excluídos conforme necessidade ou no caso de retirada de consentimento – se esse for aplicável.

O nível de segurança, no caso de servidores locais, depende, normalmente, de quem é responsável por esses. Desta forma, é importante adotar medidas robustas de segurança da informação, estabelecendo estruturas que possam proteger adequadamente os dados pessoais armazenados, mitigando as possibilidades de violação (ex.: vazamentos, comprometimento das bases de dados, dentre outros). Isso é um importante requisito em termos de proteção de dados.

Por fim, em relação ao controle de acesso, deve-se estipular medidas internas para fins de restrição aos dados. Não é recomendável que todos os(as) funcionários(as) possam acessá-los, por exemplo. Por conseguinte, recomenda-se que os dados sejam acessados na medida do estritamente necessário para o desempenho das funções desse funcionário ou funcionária, sendo o acesso irrestrito concedido, caso preciso, a poucas pessoas. Além disso, em relação aos dados pessoais sensíveis, trata-se de uma boa prática de segurança que esses dados sejam mantidos de maneira apartada, tendo também acesso restrito, dada sua sensibilidade e maior potencial para afetar a privacidade das pessoas envolvidas.

Dados armazenados em nuvem

As soluções em nuvem são sistemas de servidores interconectados que podem ser acessados remotamente via internet para finalidades como armazenamento, gestão e processamento de dados.

Uma das principais vantagens dos serviços em nuvem consiste na substituição da necessidade de manutenção de data centers físicos, tendo em vista que o armazenamento passa a ocorrer em servidores remotos de propriedade da empresa responsável pela prestação dos serviços contratados.

Além das recomendações acima, o armazenamento em nuvem pode acarretar em transferência internacional de dados, gerando obrigações adicionais aos gestores e às gestoras. Nessa situação, é importante que a empresa contratada indique em que países os serviços poderão ser prestados e quais dados pessoais serão armazenados.

No momento da contratação de empresas fornecedoras de armazenamento em nuvem, ademais, é relevante levar determinados aspectos em consideração. Assim, cabe analisar se a empresa dispõe de documentos ou políticas que versem sobre proteção de dados (ex.: termos de uso, política de privacidade, políticas de segurança da informação, dentre outros). É recomendável também que a empresa em questão esteja em conformidade com a LGPD, sendo importante a existência de registro das atividades e processos

relacionados ao tratamento de dados pessoais.

Além desses pontos, cabe destacar que a empresa deve prover segurança para a transmissão e armazenamento dos dados pessoais, observando os limites do tratamento em relação aos serviços contratados. Por fim, caso a relação contratual termine, é importante que os dados sejam transferidos adequadamente à escola ou à secretaria em questão ou à nova empresa fornecedora do serviço, devendo os dados ser eliminados pelo antigo contratado.

Dados armazenados fisicamente

Embora o armazenamento digital (seja em servidores locais ou em servidores externos através de serviços de nuvem) venha se consolidando, muitas secretarias e instituições de ensino ainda podem contar com uma série de dados armazenados fisicamente.

Nesse sentido, normas de proteção de dados são aplicáveis, sendo necessário avaliar determinadas questões, especialmente como os direitos dos(as) titulares serão garantidos. Assim, é recomendável manter os registros físicos de maneira estruturada e organizada a fim de que possíveis demandas de titulares de dados possam ser mais facilmente atendidas.

Em relação ao armazenamento, dados armazenados em arquivos físicos com informações mais sensíveis (ex.: informações médicas) devem ser arquivados em locais preferencialmente com chaves e com restrição

de acesso. Ademais, de maneira geral, é uma boa prática restringir os dados às pessoas que estritamente necessitem acessá-los. Com isso, pode-se proteger mais adequadamente a privacidade dos(as) titulares de dados e evitar que os dados sejam utilizados de maneira indevida por pessoas não autorizadas.

Quando se trata do manuseio, é importante levar em consideração as cópias de documentos que contêm dados pessoais. Isso porque, em termos de documentos físicos, é usual que tais procedimentos sejam realizados – o que pode reduzir a segurança na medida em que permite que os documentos sejam retirados de seu local de armazenamento ou eliminados de modo incorreto. Assim, sugere-se que cópias sejam realizadas para fins específicos e sejam eliminadas na medida do possível assim que seus propósitos se concretizem.

Por fim, quanto à eliminação, deve-se avaliar o tempo de retenção dos dados, estabelecendo políticas ou seguindo os prazos de normas ou leis para manutenção e eliminação dos documentos.

Além disso, é recomendável elaborar uma política de retenção de dados, estabelecendo os períodos de armazenamento para cada tipo de dado.

Também é muito importante que sejam adotados parâmetros adequados de segurança da informação durante o armazenamento dos dados pessoais. O objetivo é evitar que esses dados sejam utilizados de maneira indevida, causando danos não apenas à instituição que os armazena como também aos(às) titulares.

Abaixo, alguns questionamentos podem orientar nos processo de armazenamento.

Qual o motivo para a manutenção do dado e quando o excluir?

Dados deverão ser mantidos exclusivamente para cumprir com as finalidades informadas ao(à) titular de dados e – quando necessário – para as quais ele ou ela consentiu.

Quando se esgotarem as finalidades para as quais os dados foram armazenados ou quando o(a) titular retirar o consentimento, os dados devem ser excluídos. Adicionalmente, é possível manter dados para o cumprimento de obrigação legal ou obrigação regulatória, bem como para eventual defesa do controlador ou da controladora em processo ou procedimento judicial ou administrativo. Assim, como mencionado, caso essas obrigações legais ou regulatórias se esgotem, os dados armazenados para esses fins também deverão ser excluídos.

IMPORTANTE

Ainda não existem parâmetros que permitam identificar com mais objetividade por quanto tempo os dados devem ficar armazenados. O importante é que escolas e secretarias consigam justificar por que estão mantendo essa informação.

OK

Por quanto tempo posso manter os dados?

Os dados devem ser mantidos somente durante o período necessário para cumprir com as finalidades para as quais foram coletados. Após esse período, os dados precisam ser excluídos ou anonimizados. Isso deve ser destacado na medida em que não se pode, por exemplo, armazenar por tempo indeterminado os dados – o que é especialmente relevante no contexto educacional quando se pensa na rotatividade de estudantes.

O tempo de armazenamento vai depender também da natureza e finalidade de cada informação. Por exemplo, é necessário guardar por mais tempo o histórico escolar de estudantes do que suas fotos. Por conta disso, o período máximo de retenção nunca pode ser definido meramente com base na capacidade de armazenamento do meio utilizado.[23]

É essencial que gestores e gestoras possam justificar os motivos que levaram a secretaria a determinar o tempo de armazenamento da maneira como foi estabelecida. Isso significa que os prazos de armazenamento não podem simplesmente ser arbitrários ou definidos de forma pouco criteriosa. Lembre-se de criar critérios e padrões para os períodos pelos quais os dados serão armazenados, a menos que haja prazo preestabelecido em razão de obrigação legal ou regulatória (como

[23] Commission Nationale de l'Informatique et des Libertés (CNIL). "Vigilância por vídeo: proteção de dados pessoais nas escolas". Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaires. Acesso em: 24.07.2020.

regulamentações específicas de secretarias estaduais e municipais sobre armazenamento), a fim de que as escolhas possam ser explicadas caso seja necessário.

Destacamos que esses cuidados precisam ser tomados também em relação aos arquivos físicos. Desta forma, após o término das finalidades para as quais esses foram coletados, é importante que sejam descartados adequadamente e de forma segura (ex.: utilizar um triturador que torne os dados pessoais ininteligíveis). O descarte nunca pode ser feito de forma que permita o acesso às informações em momento posterior (ex.: simplesmente eliminar os documentos em perfeito estado, permitindo que pessoas não autorizadas possam lê-los após o descarte; usar fichas em papel com dados pessoais de estudantes como rascunho dentro da escola).

Exemplo 1: um exemplo de tempo de armazenamento pode ser observado quando se trata de sistemas de vigilância por câmeras. Nesse caso, o ideal é que o tempo de armazenamento das imagens seja curto – apenas por alguns dias, idealmente não excedendo um mês. Como regra geral, manter as imagens por esse prazo seria suficiente para realizar verificações necessárias em caso de ocorrência de quaisquer incidentes, permitindo que os procedimentos adequados sejam iniciados. Ademais, nessas situações, as imagens devem ser extraídas do dispositivo

utilizado e armazenadas apenas até que as medidas corretas sejam tomadas. Após isso, devem também ser excluídas. [24]

Exemplo 2: outro exemplo se refere a alguns dados de estudantes formados (ex.: fotos de estudantes obtidas para controle interno). Nesse caso, é importante que esses dados sejam mantidos por determinado período após a formatura, de acordo com determinações da secretaria para cada tipo de dado, caso existam pendências ou se o aluno ou a aluna desejar consultá-los. No entanto, é importante que seja estabelecido um prazo relativamente curto – entre um e dois anos, por exemplo – para que esses dados sejam excluídos. O tempo em si variará de acordo com as necessidades de cada escola ou secretaria e de acordo com a natureza do dado – sendo praticamente impossível estabelecer padrões obrigatórios. Ressalta-se também que nem todo dado deverá ser excluído, dada a existência de diversas obrigações legais e regulatórias, como aquelas emitidas pelo MEC. Por isso, é importante que se analise o caso a caso dos dados armazenados.

[24] Commission Nationale de l'Informatique et des Libertés (CNIL). "Vigilância por vídeo: proteção de dados pessoais nas escolas". Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaires. Acesso em: 24.07.2020.

O que fazer quando tenho obrigação legal em manter os dados?

É possível que determinados dados tenham de ser mantidos para fins de obrigações legais ou regulatórias (ex.: manutenção dos registros de estudantes por determinação do MEC). Nessa situação, os dados pessoais deverão ser armazenados por tempo determinado em razão de lei ou ato administrativo. Por conseguinte, deverão ser analisadas leis e normas setoriais que possam estabelecer obrigações nesse sentido – como, por exemplo, políticas estabelecidas pelo MEC e por secretarias municipais ou estaduais.

É importante ressaltar que, em decorrência da LGPD, é possível que determinados prazos sejam alterados para fins de adequação ao texto legal.

Como regra geral, caso as obrigações legais ou regulatórias cessem, é necessário excluir os dados. Em alguns casos, ainda assim, mesmo após a cessão de tais obrigações, será necessário armazenar os dados por período adicional caso esteja previsto também em lei (ex.: termo de colação de grau, atualmente compreendido como guarda permanente, conforme tabela de temporalidade).[25]

No caso de contratação de recursos educacionais digitais, em geral os dados deverão ser mantidos enquanto durar o contrato administrativo

[25] UFPEL. "Tabela de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Fim das Instituições Federais de Ensino Superior (IFES)". Disponível em: https://wp.ufpel.edu.br/scs/files/2012/04/Tabela-temporariedade-documentos-ensino-superior.pdf. Acesso em: 17.08.2020.

(normalmente, até 60 meses). Caso a secretaria ou escola deseje manter os dados gerados, deve-se considerar a necessidade de adequar tal guarda às possibilidades existentes em lei. Isso significa que os dados poderão ser mantidos, caso tal medida seja justificável. No caso de simples armazenamento, por sua vez, se ocorrer o término da relação contratual, a secretaria ou escola pode requerer a transferência dos dados existentes a si próprias ou a outra empresa fornecedora – conforme destacado na situação de armazenamento em nuvem.

Além disso, em determinadas situações, dados deverão ser mantidos pelas secretarias ou instituições de ensino para possibilitar fiscalizações de Tribunais de Contas Estaduais e outros órgãos de controle.

O que fazer com dados armazenados em plataformas digitais de terceiros?

No uso de recursos educacionais digitais, é comum que as informações sejam mantidas também nas plataformas dos terceiros. Nessas situações, é recomendável verificar o tempo e as condições de armazenamento previstas na política de privacidade e nos termos de uso da empresa parceira e certificar-se de que os dados são excluídos após o término do vínculo.

Outro ponto de atenção é a eventual disponibilização dos dados à secretaria ou escola após o término do contrato com o terceiro. Nesse caso, é necessário

assegurar que o tratamento será realizado de acordo com as leis vigentes, sendo possivelmente necessária a busca por novas justificativas para a realização das atividades perante a LGPD. Assim, se ocorrer o compartilhamento dos dados gerados e armazenados pelos terceiros com as secretarias e escolas, seria necessário justificar adequadamente o porquê desse tratamento de dados. A ação adequada a ser tomada variará de acordo com o contexto, termos do contrato com o terceiro e dados a serem disponibilizados – além de outros aspectos que se mostrarem relevantes.

Além disso, é fundamental verificar se esses terceiros adotam mecanismos de segurança apropriados para o armazenamento desses dados pessoais.

Quem é responsável por manter e, caso necessário, excluir os dados?

O responsável por manter os dados, no setor educacional, poderá variar de acordo com as obrigações postas a cada um dos envolvidos. No entanto, de maneira geral, é possível que tanto as escolas quanto as secretarias sejam responsáveis pela manutenção e, caso necessário, exclusão dos dados. Por conta disso, é provável que, em diversas situações, os dados sejam armazenados de maneira repetida – ou seja, pelas escolas e pelas secretarias, ao mesmo tempo.

No entanto, isso nem sempre acontecerá. Caso exista uma obrigação legal ou regulatória específica

à secretaria, por exemplo, poderá ocorrer de a escola não ter uma finalidade ou justificativa para armazenar aquele mesmo dado – o mesmo pode ocorrer em situação oposta, em que a escola tem obrigação, e não a secretaria.

Ademais, em caso de necessidade de exclusão, tanto as escolas como as secretarias deverão excluí-los – a menos que haja exceção posta em lei a uma das envolvidas. Por conta disso, atente-se sempre à legislação aplicável ao setor educacional e às normas setoriais.

Quem poderá acessar os dados?

Os dados devem ser acessados apenas pelas pessoas que precisam usá-los em suas atividades (ex.: profissional que detenha a competência necessária para autorizar determinada iniciativa que tenha como base dados pessoais de estudantes).

Nesse sentido, é recomendável a criação de políticas de controle de acesso aos dados por titulares de dados, servidores e servidoras públicas e outros possíveis interessados. Essas políticas deverão contemplar itens como requisitos de segurança, política relacionada à disseminação e autorização do acesso à informação, requisitos para autorização de pedidos de acesso, remoção do direito de acesso e regras para o acesso privilegiado a determinadas informações.

IMPORTANTE

Diferentes tipos de dados podem demandar níveis de acesso distintos. Desta forma, é recomendável que dados pessoais sensíveis (ex.: dados de saúde, raça, dentre outros) sejam acessados exclusivamente por pessoas autorizadas que, efetivamente, necessitam de tais informações para a realização de suas atividades.

OK

Também é importante que sejam implementadas práticas adequadas de controle de acesso com base no perfil das pessoas autorizadas (ex.: por meio do do uso de sistemas de gestão de identidade).

O ideal é que se estabeleçam níveis de acesso de acordo com as atividades de cada profissional a fim de que os dados pessoais sejam acessados apenas quando estritamente necessário. Atente-se aqui, novamente, para a importância de considerar os princípios da finalidade, necessidade e adequação.

Sempre que possível, também é recomendável a implementação de proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas em dispositivos da secretaria ou da instituição de ensino, inclusive para fins de controle de acesso (ex.: uso de criptografia e uso obrigatório de senha).

Além disso, o acesso aos dados é um direito garantido aos(às) titulares pela lei. Isso significa que estudantes e seus responsáveis legais devem ter acesso facilitado e gratuito aos dados pessoais armazenados dos quais sejam titulares. Os responsáveis legais, inclusive, em determinadas situações e a depender da idade do aluno ou aluna – normalmente menores de idade – poderão acessar seus dados em seu nome.

05.

GOVERNANÇA E PRESTAÇÃO DE CONTAS

Para assegurar a conformidade das atividades de tratamento de dados pessoais realizadas pela gestão pública educacional, também é altamente recomendável que sejam estabelecidas algumas regras de governança e boas práticas. Essas regras são responsáveis por determinar, de maneira mais objetiva, os procedimentos a serem adotados durante o tratamento de dados pessoais, e assim nortear a atuação de gestores e gestoras de acordo com a legislação e com as boas práticas em termos de proteção de dados pessoais.

A adoção de regras de governança e boas práticas não apenas é fomentada pela LGPD (que possui uma seção específica destinada a esse tema), mas também pode auxiliar na atenuação de eventuais penalidades em caso de tratamento indevido de dados pessoais[26]. A seguir, apresentamos algumas sugestões de regras de governança e boas práticas que podem ser adotadas no setor educacional. Para tanto, além de recomendações mais genéricas, indicamos também uma série de referências que se mostram mais recorrentes em situações como a aquisição de recursos educacionais digitais, com base no fluxo do Toolkit de Seleção e Aquisição de Tecnologias Educacionais desenvolvido pelo CIEB[27].

[25] Confederação Nacional da Indústria (CNI). "LGPD: o que a sua empresa precisa saber". 2020. Disponível em: https://bucket-gw-cni-static-cms-si.s3.amazonaws.com/media/filer_public/d6/29/d6297686-923a-4f69-8d4b-ff81bb4e8eb8/lgpd_o_que_sua_empresa_precisa_saber.pdf. Acesso em: 31.08.2020.

[26] CIEB. "Toolkit de Seleção e Aquisição de Tecnologias Educacionais". Disponível em: https://toolkit.plataformaedutec.com.br/. Acesso em 08.09.2020.

01.

QUAIS CUIDADOS COM DADOS PESSOAIS DEVEM SER OBSERVADOS NA AQUISIÇÃO DE RECURSOS EDUCACIONAIS DIGITAIS?

Recomendações gerais

Em linhas gerais, é recomendável que todas as aquisições sejam feitas com parceiros confiáveis, que desempenhem suas atividades de maneira alinhada com as normas de proteção de dados pessoais.

Exemplo: Para a contratação de empresas que prestem serviços de armazenamento de dados em nuvem, recomenda-se avaliar, durante a pesquisa de mercado e de preço, quais são reconhecidas por seguir padrões rigorosos de privacidade.

Nessas contratações, é importante que os seguintes pontos sejam observados por gestores e gestoras:

O termo de referência e o contrato devem **definir as responsabilidades** de cada uma das partes em questões relacionadas ao tratamento de dados pessoais. Essa atribuição de responsabilidades vai depender do papel das partes no tratamento dos dados pessoais (em geral, a secretaria/escola atuará como controladora e a empresa fornecedora contratada, como operadora).

Os dados pessoais não devem ser utilizados para **finalidades** distintas daquelas previstas no termo de referência e contrato.

As partes do contrato devem se comprometer a cumprir as **obrigações legais e regulatórias** relacionadas à proteção de dados pessoais, incluindo, mas não se limitando à LGPD.

A empresa e/ou profissional contratado(a) deve adotar **medidas adequadas de segurança da informação** durante o tratamento dos dados pessoais.

A empresa/profissional contratado(a) deve se comprometer a auxiliar a secretaria e/ou escola (nos casos em que estas últimas atuarem como controladoras), quando necessário, a viabilizar a efetivação dos **direitos dos(as) titulares**.

Recomendações específicas

A seguir, apresentamos algumas recomendações relacionadas à proteção de dados a serem observadas nas principais etapas da aquisição dos recursos tecnológicos.

Fase 1
Planejamento para aquisição de tecnologia

O que fazer?

Durante o planejamento e identificação de demandas de tecnologia educacional, verificar se esse tipo de tecnologia demanda a coleta e uso de dados pessoais de estudantes/responsáveis, servidores e servidoras públicas e/ou outros titulares relacionados à instituição de ensino/secretaria.

Em caso positivo, verificar quais dados pessoais poderão ser coletados (incluindo a verificação de necessidade de coleta de dados pessoais sensíveis).

Após verificar se há uso de dados pessoais e quais dados pessoais são utilizados no funcionamento da tecnologia, é necessário verificar se esse uso pode trazer riscos aos(às) titulares dos dados pessoais, e se a aquisição desse tipo de tecnologia é de fato necessária para o desenvolvimento da atividade pretendida.

Como fazer?

Verificar os atributos da tecnologia, suas funcionalidades e aplicações, além de analisar a política de privacidade e os **termos de uso**.

Os **termos de uso** são um documento com informações sobre a interação entre a empresa fornecedora da tecnologia e o usuário e a usuária, a partir da descrição de seus produtos e/ou serviços e das condições estabelecidas para o seu uso. Esse documento é relevante especialmente por (i) permitir às pessoas um fácil acesso sobre as condições de uso dos produtos e/ou serviços da empresa fornecedora da tecnologia, e (ii) indicar, de maneira mais expressa, para clientes e demais atores do mercado (como concorrentes e reguladores), que as práticas da empresa fornecedora da tecnologia são adequadas em relação à legislação e às melhores práticas de proteção de dados pessoais.

Já a **política de privacidade** é um documento com informações sobre as atividades de tratamento de dados pessoais realizadas pela empresa fornecedora da tecnologia durante a interação de usuários e usuárias com os seus produtos e/ou serviços. Esse documento deve indicar, de forma detalhada, as atividades de tratamento da empresa fornecedora da tecnologia em relação aos dados pessoais de titulares externos (ex.: clientes, consumidores/as, usuários/as, entre outros), de forma a oferecer informação sobre o tratamento de seus dados (coleta, armazenamento,

compartilhamento, finalidade) e sobre o exercício dos seus direitos nos procedimentos internos da empresa (acesso, correção, deleção, portabilidade, bloqueio, entre outros). Sua relevância se deve ao fato de:

1. Permitir aos usuários e usuárias um fácil acesso às condições pelas quais os seus dados pessoais são tratados pela empresa fornecedora da tecnologia e

2. Informar de maneira mais expressa para clientes e demais atores do mercado (como concorrentes e reguladores) a sua adequação em termos de proteção de dados pessoais.

Fase 2
Definição da tecnologia a ser adquirida

O que fazer?

Estabelecer como um dos requisitos técnicos a adequação do produto à LGPD.

- Verificar quais dados são coletados pela ferramenta ao longo do seu funcionamento (dados pessoais e dados pessoais sensíveis).

- Verificar se a empresa fornecedora se compromete a não compartilhar dados pessoais posteriormente ou usá-los fora do necessário para fornecer o produto ou serviço.

- Verificar se a empresa fornecedora se compromete a adotar mecanismos de segurança robustos, que assegurem uma maior proteção aos dados pessoais tratados.

- Verificar se existe a possibilidade de anonimização dos dados pessoais tratados pela empresa fornecedora durante o oferecimento da tecnologia.

- Verificar se é realizado o tratamento de dados pessoais com base em decisões tomadas de forma unicamente automatizada por parte da fornecedora.

- Verificar se a fornecedora cria perfis de estudantes para além das finalidades educacionais.

- Verificar se a ferramenta mostra anúncios de propaganda aos usuários e usuárias.

IMPORTANTE

O comprometimento da empresa/profissional responsável pela tecnologia com a proteção de dados pessoais deve ser considerado um **diferencial competitivo** para auxiliar na decisão de gestores e gestoras educacionais quanto à aquisição da tecnologia. Isso porque, mais do que optar por parceiros e parceiras antigas ou empresas que apresentem um orçamento menor, é importante avaliar os potenciais riscos que incidentes relacionados a tratamento indevido de dados pessoais – especialmente se envolver dados pessoais de estudantes – podem gerar à secretaria e/ou à instituição de ensino (como incidência de multas da LGPD, prejuízo para a imagem da rede de ensino e riscos aos titulares de dados, especialmente a estudantes).

OK

Exemplo: no caso de contratação de tecnologia que utilize dados de menores, uma sugestão é privilegiar empresas que adotem uma abordagem de *children's-rights-by-design*, ou seja, empresas que privilegiem e promovam o melhor interesse da criança em ambiente digital, inclusive desde o momento de desenvolvimento e concepção dessas tecnologias.[28]

[28] Criança e Consumo. "Criança e Consumo contribui com Novo Comentário Geral sobre Direitos das Crianças em Relação ao Ambiente Digital da ONU". Disponível em: https://criancaeconsumo.org.br/noticias/crianca-e-consumo-contribui-com-novo-comentario-geral-sobre-direitos-das-criancas-em-relacao-ao-ambiente-digital-da-onu/. Acesso em: 10.09.2020.

Fase 3
Decisão sobre a viabilidade da aquisição

O que fazer?

Verificar se a tecnologia a ser adquirida cumpre os requisitos mencionados na Fase 2 “Definição da tecnologia a ser adquirida”.

Caso não cumpra, é necessário avaliar os riscos à privacidade e à proteção de dados pessoais que podem ser causados aos(às) titulares em decorrência do uso da ferramenta.

Verificar as salvaguardas e medidas de mitigação que podem ser adotadas quanto a esses riscos (ex.: possibilidade de limitar a retenção dos dados pela empresa, viabilidade/necessidade de coleta de consentimento para uso dos dados pessoais).

Como fazer?

Elaboração de um relatórios de impacto de proteção de dados (ver abaixo ponto sobre relatório de impacto de proteção de dados).

DICA

A análise dos riscos pode ser realizada junto ao Estudo Técnico Preliminar, por meio do qual são descritos os riscos a possibilidade de ocorrência, os impactos e as ações de mitigação. Nessa situação, gestores e gestoras educacionais devem avaliar quais atividades de tratamento de dados realizadas com a ferramenta tecnológica e verificar a possibilidade de ocorrência de riscos como, por exemplo:

1. Riscos à privacidade de estudantes pela ausência de clareza sobre o uso de dados pela ferramenta;

2. Risco quanto ao uso de dados pessoais sensíveis;

3. Risco de vazamento de dados. Essa avaliação pode ser feita, conforme já mencionado, a partir da política de privacidade e termos de uso da ferramenta. A análise de impacto desses riscos vai variar conforme o tipo de dado tratado (dado pessoal, dado pessoal sensível) e dos(as) titulares (se forem crianças menores de 12 anos os impactos devem ser considerados maiores), além da reputação do desenvolvedor ou desenvolvedora (por exemplo, caso já tenha ocorrido algum incidente prévio de segurança, o risco pode ser considerado mais alto).

OK

Fase 4
Termo de Referência

O que fazer?

O Termo de Referência é o documento que deve conter os elementos que caracterizem o objeto da contratação pública. Esse Termo de Referência é elaborado a partir de estudos técnicos preliminares e demais documentos produzidos durante o planejamento da aquisição, e deve contar com um nível de precisão adequado. Sua elaboração é obrigatória para qualquer aquisição, seja ela feita por meio de processo licitatório, contratação direta (dispensa ou inexigibilidade) ou inclusive por adesão a ata de registro de preços.

Dentre os elementos necessários e suficientes para caracterizar a precisão do Termo de Referência, deve constar como requisito para a aquisição a adequação da empresa interessada aos requisitos da LGPD.

Como fazer?

Incluir, no Termo de Referência, requisitos relacionados a proteção dos dados pessoais a fim de ajudar na seleção de empresas fornecedoras mais adequadas no que diz respeito à proteção de dados pessoais. O Anexo I contém modelos de cláusulas de proteção de dados pessoais e orientações sobre o que levar em conta ao redigir o Termo de Referência.

SAIBA MAIS

Fase 5
Elaboração do contrato

O que fazer?

Estabelecer a responsabilidade das partes no tratamento de dados pessoais, indicando quem é controlador e quem é operador.

Estabelecer no contrato instruções sobre as atividades de tratamento de dados que deverão ser realizadas pela empresa, incluindo requisitos de armazenamento, exclusão ao término do vínculo e, quando viável, impedindo o uso de dados para outras finalidades além daquela objeto da contratação (mais informações sobre as diretrizes para cláusulas contratuais são apresentadas no Anexo I deste Manual).

SAIBA MAIS

ESTUDO DE CASO

CONTRATAÇÃO DE FERRAMENTA TECNOLÓGICA DE AVALIAÇÃO *ONLINE*

Uma **secretaria de educação** de determinado município avalia contratar uma ferramenta inovadora de avaliação *online* para aplicação na rede de ensino pública municipal. A ferramenta coleta uma série de dados de estudantes, como nome, idade, informações de contato, conteúdos produzidos, fotos dos estudantes, registros de imagem e voz dos estudantes, dados de navegação (IP do dispositivo, cookies, etc), além de criar perfis de alunos e alunas baseados em seu desempenho.

A empresa fornecedora da tecnologia retém esses dados para desenvolver novos produtos e serviços, além de enriquecê-los a partir de outras fontes de informação (e.g. dados tornados públicos em redes sociais). No âmbito dessas atividades, a empresa oferece serviços de venda de base de dados para empresas parceiras que queiram desenvolver seus produtos, sem especificar como esses terceiros podem usar essas informações.

Considerando a essencialidade da ferramenta e sua característica inovadora, a secretaria municipal decide prosseguir com a contratação e, com o auxílio do encarregado ou da encarregada do município, faz uma avaliação dos riscos aos(às) titulares dos dados. A partir da análise da ferramenta, são apontados os seguintes riscos: (i) criação de perfis de estudantes; (ii) uso de dados biométricos; (iii) enriquecimento de bases de dados com outras fontes; e (iv) compartilhamento com terceiros.

A partir dos riscos apresentados, o encarregado ou a encarregada, junto com a secretaria, avalia quais medidas de mitigação devem ser tomadas para proteção dos(as) titulares dos dados e em qual momento da contratação. Assim, foram apresentadas as seguintes recomendações para serem incluídas no termo de referência:

Limitar a criação dos perfis com dados educacionais (coletado no uso do/a titular na ferramenta como os conteúdos produzidos, tempo para elaboração da tarefa, entre outros);

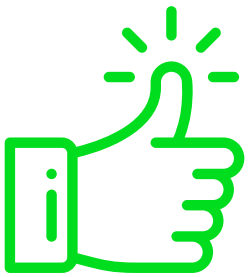
- Restringir o uso dos perfis para outros fins fora do escopo educacional;
- Restringir as atividades relacionadas ao enriquecimento das bases de dados;
- Restringir o compartilhamento de dados pessoais com terceiros ao necessário para o uso da ferramenta;
- Estimular a manutenção apenas de dados anonimizados.

Ao momento da contratação, a secretaria, junto ao encarregado ou encarregada, elabora cláusulas de proteção de dados a serem inseridas no contrato, nos seguintes termos:

- Determinação de que as partes se comprometerão a **cumprir a legislação aplicável a proteção de dados pessoais**, com destaque para a LGPD;
- Determinação do(a) desenvolvedor(a) como operador(a) dos dados, limitando suas atividades de tratamento às instruções fornecidas pela secretaria/instituição de ensino;
- Limitação das atividades de tratamento ao contexto educacional, restringindo a reutilização dos dados, compartilhamento ou enriquecimento dos dados com outras

fontes;

- Determinação do(a) desenvolvedor(a) como responsável pela segurança no armazenamento dos dados sob sua guarda, incluindo garantias de confidencialidade e sigilo aos colabores que têm acesso aos dados;
- Colaboração com a efetivação dos direitos dos(as) titulares quando solicitado;
- Exclusão dos dados ao término do contrato ou anonimização das informações.
- No caso de anonimização, determinação indicando a necessidade de o(a) desenvolvedor(a) divulgar a técnica utilizada para a anonimização dos dados;
- Determinação de que o(a) desenvolvedor(a) deve manter registro das atividades de tratamento realizadas em nome da secretaria;
- Indicação de necessidade de comunicação, em prazo razoável, em caso de vazamento de dados.



02.

BOAS PRÁTICAS E RECOMENDAÇÕES

Criar uma estrutura de governança em proteção de dados pessoais

Criar uma estrutura de governança dentro da **secretaria de educação** e/ou escola, com o propósito de conduzir as atividades relacionadas à adequação à LGPD, auxiliar a equipe de educação em sua obrigação com dados, monitorar as leis e regulamentos aplicáveis e o seu cumprimento, e gerenciar atividades internas de proteção de dados, treinamento e auditorias internas.

SAIBA MAIS

Essa estrutura pode ser centralizada no encarregado ou encarregada (ver ponto 4 acima) que, pela lei, deve orientar a gestão, a diretoria, a docência e demais áreas do serviço público a respeito dos cuidados necessários para proteger os dados tratados pela secretaria ou escola.

Quando necessário, recomendamos também que a secretaria de educação e/ou escola consultem profissionais especializados no tema (ex.: advogados e advogadas especialistas em proteção de dados, técnicos e técnicas de segurança da informação) a fim

de construir uma estrutura de governança mais robusta e adequada à legislação aplicável.[29]

Mapear e registrar todas as operações de tratamento de dados

Elaborar um mapeamento com a descrição detalhada de todas as operações realizadas com dados pessoais na rede de ensino. Uma forma de começar a realizar esse mapeamento pode ser desenhando o ciclo de vida dos dados a partir de três pontos:

Dados recebidos: informações repassadas por outras pessoas ou instituições (como autoridades locais) para a secretaria ou escola.
Dados coletados e criados na rede de ensino: dados coletados de estudantes em controle de presença, históricos escolar, dados comportamentais.
Dados repassados a outros: dados repassados dentro da rede de ensino (ex.: entre escolas ou entre escola e secretaria), dados repassados para uma autoridade local, para familiares de estudantes, etc.

Com base nessas informações, gestores e gestoras devem identificar todos os dados tratados pela secretaria ou instituição de ensino (ver ponto 2: exemplo de dados pessoais no setor educacional), verificar onde eles se encaixam no fluxo dos dados (dados recebidos, coletados ou repassados) e rever a adequação desses procedimentos com base na LGPD. [30]

[29] BORELLI, Alessandra. "É pra já! A proteção de dados de crianças e adolescentes não pode esperar". Julho de 2020. Disponível em: https://cdn.asp.events/CLIENT_Ascentia_4E961A52_5056_B739_54289B84DF34E888/sites/BettBrasil20Port/media/E%CC%81%20pra%20ja%CC%81%20-%2025%20agosto.pdf. Acesso em: 31.08.2020.

[30] Ibid.

Engajar os(as) profissionais de TI (Tecnologia da Informação) que atuam na rede de ensino a documentar e mapear em quais sistemas computacionais os dados são utilizados.

Atualizar normas e políticas para o tratamento de dados pessoais

Mapear normas e documentos que envolvem o tratamento de dados, e verificar a adequação dessas normas e documentos à LGPD.

- **Exemplo 1:** verificar se todos os dados solicitados nas fichas cadastrais de matrícula são necessários, bem como incluir cláusulas de consentimento nessas fichas, nos casos em que o consentimento for necessário.
- **Exemplo 2:** atualizar políticas de armazenamento e retenção dos dados e de controle de acesso.
- **Exemplo 3:** revisitar as políticas para elaboração de ficha de estudantes e os dados contidos nessas fichas.
- **Exemplo 4:** revisar e/ou elaborar políticas de segurança da informação e de gestão de incidentes a fim de adequá-las à LGPD em relação às práticas que envolvem o tratamento de dados pessoais.

Destacamos o fato de que alguns órgãos e entidades públicos já apresentam diretrizes internas para adequação do tratamento dos dados pessoais.

Exemplo: O Decreto Estadual nº 49.265, de 6 de agosto de 2020, que institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual de Pernambuco em consonância com a LGPD.[31]

Atualizar instrumentos contratuais com profissionais da rede que são titulares de dados

Verificar os instrumentos contratuais firmados com titulares de dados (ex: docentes, servidores e servidoras públicas da rede de ensino), principalmente os profissionais que podem tomar decisões em relação aos dados pessoais, e estabelecer disposições relacionadas à proteção de dados, disciplinando as condições para o tratamento de dados e as responsabilidades das partes nas atividades de tratamento.

[31] Governo do Estado de Pernambuco. Decreto Estadual nº 49.265, de 6 de agosto de 2020. Disponível em: https://legis.policiacivil.pe.gov.br/L2/resources/docs/3dca01e3b7c6c033c39d11fd7b3019aa.pdf. Acesso em: 31.08.2020.

Exemplo: Nos contratos de trabalho firmados com profissionais da secretaria, recomendamos que haja cláusulas específicas relacionadas a questões como quais os seus direitos enquanto titulares de dados pessoais, e quais as suas responsabilidades relacionadas ao tratamento de dados pessoais durante o exercício das suas atividades profissionais.

Realizar ciclos de conscientização sobre proteção de dados pessoais

Levantar discussões com o propósito de conscientizar gestores e gestoras educacionais, servidores e servidoras públicas da rede de ensino e demais envolvidos que têm contato com dados pessoais sobre a importância da temática da privacidade.

Relacionar a proteção de dados com a proteção de crianças e adolescentes, a fim de oferecer abordagens educacionais que permitam uma maior proximidade ao tema da privacidade no dia a dia de educadores e educadoras.

Incentivar que a comunidade esteja engajada e articulada com preocupações relacionadas à privacidade no ambiente escolar.

1. Profissionais da educação devem estar cientes dos riscos relacionados ao uso indevido de informações pessoais de estudantes e suas responsabilidades em caso de vazamento de dados.

2. Profissionais da educação devem participar de discussões sobre identificação e mitigação de riscos relacionados à coleta, ao uso e ao armazenamento de dados.

Promover eventos direcionados à disseminação da cultura da privacidade e da proteção de dados entre profissionais da educação.

Oferecer formação aos profissionais da secretaria e instituições de ensino

Oferecer diferentes ciclos de formação a funcionários e funcionárias e a educadores e educadoras, a depender do cargo que ocupam, relacionados a boas práticas em termos de proteção de dados pessoais.

1. **A toda equipe:** oferecer formação a toda equipe voltada a conscientizá-la sobre o tema da privacidade e proteção de dados, além de instruí-la sobre os cuidados básicos no uso de dados pessoais (ex.: cuidados no manuseio de documentos físicos que contenham dados pessoais de estudantes para evitar que possam ser utilizados de forma indevida por terceiros; boas práticas de segurança da informação,

como estimular a troca periódicas de senhas de acesso a sistemas da secretaria/escola e recomendar a não abertura de e-mails suspeitos). Além disso, recomenda-se também a divulgação de cartilhas e orientações gerais sobre o tema da privacidade e proteção de dados.

2. **A funcionários e funcionárias que têm autoridade para criar, coletar e armazenar dados e decidir quando tratar determinados dados:** oferecer formações sobre conceitos mais técnicos relacionados a proteção de dados, como bases legais aplicáveis, requisitos para tratamento, formas de mitigação de risco no tratamento de dados, preocupações com o uso de tecnologia que podem usar dados pessoais, formas seguras de armazenamento, entre outros.

3. **A encarregados e encarregadas:** permitir a realização de cursos, treinamentos, preparação para obtenção de certificados, dentre outras categorias de formação semelhantes, e fornecer recursos necessários, como equipe de apoio e recursos financeiros e de tecnologia da informação suficientes, para que as pessoas que realizam essa função sejam capazes de desempenhar apropriadamente suas tarefas, o que envolve, por exemplo: receber solicitações feitas por titulares de dados pessoais e garantir o devido encaminhamento a essas solicitações, ou orientar servidores e servidoras públicas sobre boas práticas em termos de proteção de dados pessoais.

4. **A gestores e gestoras e ao corpo docente:** sempre que possível, fomentar iniciativas pedagógicas que abordem o tema da proteção de dados pessoais junto aos(às) estudantes (ex.: integração do tema no conteúdo curricular de outras disciplinas[32]; realização de dinâmicas sobre como usar a internet de forma segura).

Elaborar relatórios de impacto de proteção de dados

Relatórios de impacto de proteção de dados são ferramentas para ajudar a identificar e mitigar riscos de proteção de dados.

O relatório de impacto consiste em um documento com as seguintes informações: (i) descrição dos tipos de dados coletados; (ii) metodologia utilizada para coleta; (iii) análise das medidas adotadas para mitigar os riscos aos titulares. Esse documento vai ser necessário quando as atividades de tratamento resultam em riscos aos direitos e liberdades dos titulares.

[32] BORELLI, Alessandra. "É pra já! A proteção de dados de crianças e adolescentes não pode esperar". Julho de 2020. Disponível em: https://cdn.asp.events/CLIENT_Ascentia_4E961A52_5056_B739_54289B84DF34E888/sites/BettBrasil20Port/media/E%CC%81%20pra%20ja%CC%81%20-%2025%20agosto.pdf. Acesso em: 31.08.2020.

Exemplo: uma escola pretende usar uma tecnologia de reconhecimento facial para controlar a presença de estudantes. Nesse caso, considerando

1. a possibilidade de serem tratados dados pessoais sensíveis (biometria facial);

2. o fato de os titulares serem crianças e adolescentes; e

3. a possibilidade de retenção das informações por terceiros (desenvolvedor da tecnologia), existem riscos consideráveis aos(às) titulares dos dados devido ao uso da tecnologia.

Nesse contexto, é recomendável elaborar um relatório de impacto de proteção de dados, avaliando os riscos no uso dessa ferramenta e as potenciais medidas de mitigação a serem adotadas pela escola. Caso a escola, mesmo diante dos riscos, opte por usar a tecnologia, é recomendável também pensar em formas de mitigação desses riscos, tais como: impedir que o fornecedor da tecnologia guarde e use as informações biométricas; colete o consentimento dos(as) estudantes e dos familiares para usar a tecnologia; restrinja o uso da ferramenta a estudantes maiores de 12 anos, entre outras.

06.

CONSIDERAÇÕES FINAIS

Em meio a um contexto no qual os dados pessoais adquirem crescente relevância no cotidiano do ensino público, a leitura deste Manual pode ser extremamente valiosa para gestores e gestoras educacionais, especialmente diante do seu objetivo de apresentar, de maneira didática e contextualizada, as principais noções sobre proteção de dados pessoais nesse ambiente e as cautelas recomendadas durante o tratamento de dados pessoais.

Além disso, as obrigações para o tratamento de dados pessoais trazidas pela LGPD estão longe de representar um mero entrave ao desenvolvimento de atividades na gestão pública educacional, especialmente em termos de contratação de novas tecnologias. Pelo contrário: a LGPD surge como um parâmetro extremamente enriquecedor não apenas para assegurar maior proteção aos titulares de dados pessoais (que terão os seus direitos garantidos pelos agentes de tratamento), mas também para proporcionar maior segurança para as secretarias e instituições de ensino (por exemplo, ao possuir critérios mais robustos para seleção e contratação de parceiros confiáveis em termos de proteção de dados e segurança da informação).

Com isso, espera-se não apenas desmistificar diversas questões relacionadas ao uso de dados pessoais, mas também auxiliar a incorporação de medidas de proteção de dados pessoais no dia a dia das atividades de gestores e gestoras.

07.

REFERÊNCIAS

Agencia Española de Protección de Datos (AEPD). ”Guía para Centros Educativos”. p. 28. Disponível em: http://tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf. Acesso em: 23.07.2020.

Agrupamento de Escolas Dr. Serafim Leite. Política de Privacidade e Proteção de Dados Pessoais. Disponível em: http://essl.pt/images/Modulos_pag_principal/RGPD_AESL_signed.pdf. Acesso em 10.08.2020.

BORELLI, Alessandra. “É pra já! A proteção de dados de crianças e adolescentes não pode esperar”. Julho de 2020. Disponível em: https://cdn.asp.events/CLIENT_Ascentia_4E961A52_5056_B739_54289B84DF34E888/sites/BettBrasil20Port/media/E%CC%81%20pra%20ja%CC%81%20-%2025%20agosto.pdf. Acesso em: 31.08.2020.

CIEB. “O papel das práticas pedagógicas inovadoras mediadas por tecnologia”. Disponível em: https://cieb.net.br/o-papel-das-praticas-pedagogicas-inovadoras-mediadas-por-tecnologia/#:~:text=S%C3%A3o%20seis%20os%20modelos%20de,ensino%20h%C3%ADbrido%3A%20rota%C3%A7%C3%A3o%20por%20esta%C3%A7%C3%B5es. Acesso em 30.07.2020.

_____. “Aprendizagem Remota em Tempos de Pandemia”. Disponível em: https://pandemia.cieb.net.br/. Acesso em 10.08.2020.

_____. “Guia de Implementação de Estratégias de Aprendizagem Remota”. Disponível em: https://aprendizagem-remota.cieb.net.br/guia. Acesso em 10.08.2020.

_____. “Pesquisa: Planejamento das Secretarias de Educação do Brasil para Ensino Remoto”. Disponível em: https://cieb.net.br/wp-content/uploads/2020/04/CIEB-Planejamento-Secretarias-de-Educac%C3%A3o-para-Ensino-Remoto-030420.pdf. Acesso em 30.07.2020.

_____. “Toolkit de Seleção e Aquisição de Tecnologias Educacionais”. Disponível em: https://toolkit.plataformaedutec.com.br/. Acesso em 08.09.2020.

Confederação Nacional da Indústria (CNI). “LGPD: o que a sua empresa precisa saber”. 2020. Disponível em: https://bucket-gw-cni-static-cms-si.s3.amazonaws.com/media/filer_public/d6/29/d6297686-923a-4f69-8d4b-ff81bb4e8eb8/lgpd_o_que_sua_empresa_precisa_saber.pdf. Acesso em: 31.08.2020.

Commission Nationale de l’Informatique et des Libertés (CNIL). “Vigilância por vídeo: proteção de dados pessoais nas escolas”. Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaires. Acesso em: 24.07.2020.

Escola Secundária João Gonçalves Zarco. Política de Privacidade e Proteção de Dados Pessoais. Disponível em: https://www.zarco.pt/site/index.php/polprivacidade/. Acesso em 10.08.2020.

Escolas Exponenciais. “Como adaptar sua escola para o cumprimento da nova Lei de Dados Pessoais?” Disponível em: https://escolasexponenciais.com.br/inovacao-e-gestao/como-adaptar-sua-escola-para-o-cumprimento-da-nova-lei-de-dados-pessoais/. Acesso em 03.09.2020.

Garante Privacy. “Autoridade italiana publica esclarecimentos sobre publicação de notas em contexto escolar”. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9367295. Acesso em: 22.07.2020.

Governo do Estado de Pernambuco. Decreto Estadual nº 49.265, de 6 de agosto de 2020. Disponível em: https://legis.policiacivil.pe.gov.br/L2/resources/docs/3dca01e3b7c6c033c39d11fd7b3019aa.pdf. Acesso em: 31.08.2020.

Governo do Estado do Rio de Janeiro. Lei nº 8.973/2020, de 10 de agosto de 2020. Disponível em: https://www.legisweb.com.br/legislacao/?id=399821. Acesso em 30.07.2020.

Governo Federal. “Guia de Boas Práticas para Implementação na Administração Pública Federal”, p. 9. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 21.08.2020.

ICO (Information Comissioner's Office. "WP29 Guidelines on Data Protection Officers ("DPOs"); ICO Data protection officers". Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/. Acesso em 01.09.2020.

Internetlab. "Lei Geral de Proteção de Dados e a tutela dos dados pessoais de crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais". Disponível em: https://bit.ly/33BvJQy. Acesso em: 28.07.2020.

Instituto de Tecnologia e Sociedade (ITS). "Lei Geral de Proteção de Dados Pessoais (LGPD) e Setor Público". 2020. Disponível em: https://itsrio.org/pt/publicacoes/lei-geral-de-protecao-de-dados-pessoais-lgpd-e-setor-publico/. Acesso em 03.09.2020.

Ministério da Educação. "MEC lança aplicativo para dar transparência a dados educacionais e financeiros de escolas". Disponível em: http://portal.mec.gov.br/component/content/article?id=86531. Acesso em: 31.08.2020.

Ministério da Educação. "Informações sobre a Política de Privacidade - Id Estudantil". Disponível em: http://idestudantil.mec.gov.br/como-podemos-ajudar/guia-da-id-estudantil/31-informacoes-sobre-a-politica-de-privacidade. Acesso em 03.09.2020.

Pinheiro. Patricia Peck. "A LGPD aplicada ao setor da educação". 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/educacao-lgpd#:~:text=%C3%89%20um%20ambiente%20aberto%20ao,dados%20dos%20cidad%C3%A3os%20do%20pa%C3%ADs. Acesso em 03.09.2020.

Secretaria Municipal de Educação do Município de São Paulo. "Formulário de Pré-Cadastro Infantil". Disponível em: https://cadastroinfantil.sme.prefeitura.sp.gov.br/. Acesso em: 06.08.2020.

UFPEL. "Tabela de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Fim das Instituições Federais de Ensino Superior (IFES)". Disponível em: https://wp.ufpel.edu.br/scs/files/2012/04/Tabela-

temporariedade-documentos-ensino-superior.pdf. Acesso em: 17.08.2020.

VALENTE, Patricia Pessôa; MICALI, Giovanna. LGPD e inovação no setor público: o caso das edutechs. in DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coord). LGPD e Administração Pública: uma análise ampla dos impactos. São Paulo: Revista dos Tribunais, 2020.

08.

ANEXOS

Anexo I – Modelo de cláusulas de proteção de dados pessoais para Termos de Referência e Contratos

Seja em Termos de Referência ou contratos firmados por gestores e gestoras públicas, é importante que dispositivos relacionados à proteção de dados pessoais estejam presentes. Nesse sentido, apresentamos a seguir alguns exemplos de temas que devem ser abordados:

- Determinação de que as partes se comprometerão a **cumprir a legislação aplicável à proteção de dados pessoais,** com destaque para a LGPD.
- **Divisão de responsabilidade entre as partes** em questões relacionadas ao tratamento de dados pessoais.
- Indicação da necessidade de realização do **tratamento** dos dados pessoais exclusivamente de acordo com as instruções documentadas da secretaria/instituição de ensino, **para finalidade de cumprimento do Termo/contrato.**
- Indicação da necessidade de implementação de **medidas de segurança da informação** para assegurar a proteção dos dados.
- Indicação da necessidade de **colaboração com a efetivação dos direitos dos titulares** de dados pessoais, quando solicitado.
- Indicação da necessidade de **manutenção de registros** por escrito das atividades de tratamento de dados pessoais realizadas.
- Indicação da necessidade de comunicação, de maneira imediata ou em até 24 horas do momento em que tomar conhecimento, sobre qualquer **tratamento não autorizado ou ilícito dos dados pessoais** (ex.: acesso não autorizado, vazamento de dados, etc).

- Indicação da necessidade de **permissão e cooperação com investigações** de incidentes, realizadas pela secretaria/instituição de ensino ou por terceiros por ela contratados.

Termos de referência

- **Exemplo 1:** No item dos Termos de Referência relativo a "Requisitos da Contratação", uma sugestão seria a seguinte: *"A solução a ser contratada deverá atender aos seguintes requisitos técnicos: [...] Estar adaptada aos requisitos da Lei n° 13.709/2020 (Lei Geral de Proteção de Dados ou "LGPD")".*

- **Exemplo 2:** Além disso, nos "Critérios de Habilitação" dos Termos de Referência, pode haver solicitação de demonstração de conformidade com a LGPD por parte do(a) proponente, nos seguintes termos: *"A empresa que participar do processo de contratação deverá apresentar documentação que ateste a sua habilitação em termos de adequação à LGPD, que consistirá em: [atestado de qualificação técnica em trabalhos prestados em LGPD / indicação de certificações como as normas ISO, além de outras certificações pertinentes relacionadas a proteção de dados e segurança da informação]."*

Contratos

- **Exemplo 1:** Nos casos em que a secretaria/instituição de ensino atuar como controladora dos dados pessoais e a empresa contratada, como operadora, a determinação do papel de cada uma das partes enquanto agentes de tratamento de dados pessoais é fundamental. Nesse sentido, uma possível cláusula seria a seguinte: *"Para viabilizar a prestação dos serviços conforme previsto neste Contrato, a Contratante confirma que,*

durante o desenvolvimento das suas atividades de tratamento de dados pessoais relacionados à execução do Contrato, atuará como controladora, sendo responsável pela definição das decisões referentes ao tratamento de dados pessoais. Por outro lado, a Contratada confirma que atuará como operadora dos dados pessoais, devendo tratá-los estritamente de acordo com as orientações expressas da Contratada para fins de cumprimento do presente Contrato.".

- **Exemplo 2:** Também é essencial que as partes estabeleçam as responsabilidades para a viabilização dos direitos dos(as) titulares cujos dados serão tratados em decorrência do Contrato, como na seguinte sugestão: *"A Contratada se compromete a colaborar com a Contratante na efetivação dos direitos dos(as) titulares dos dados pessoais quando solicitada, de acordo com a legislação aplicável.".*
- **Exemplo 3:** Outra questão fundamental a ser abordada nos Contratos envolve o comprometimento da parte contratada com a segurança da informação no tratamento dos dados pessoais, que poderia ser indicado da seguinte maneira: *"A Contratada se compromete a implementar medidas de segurança, técnicas e administrativas adequadas para garantir um nível de segurança efetivo para a proteção dos dados pessoais contra acessos não autorizados e incidentes envolvendo destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito desses dados pessoais".*

Observação

Tanto nos Termos de Referência quanto nos Contratos elaborados e firmados pelas secretarias/instituições de ensino, é necessário validar as cláusulas a serem implementadas junto à respectiva **assessoria jurídica competente**, especialmente para verificar a adequação dessas cláusulas às particularidades dos Termos de Referência e Contratos nos quais se aplicam.

Anexo II – Modelo de política de privacidade

A Política de Privacidade é um documento que reúne informações sobre as atividades de tratamento de dados pessoais realizadas durante a interação do usuário ou usuária com determinados produtos e/ou serviços. No âmbito da gestão educacional pública, é importante que as secretarias de educação indiquem informações relacionadas às atividades de tratamento de dados pessoais, como forma de coleta dos dados e indicação dos direitos dos(as) titulares desses dados. Além disso, a Política de Privacidade deve ser disponibilizada publicamente, de preferência em local de fácil acesso aos usuários e usuárias (ex.: no rodapé do website da **secretaria de educação**).

Secretarias de educação estaduais e municipais frequentemente possuem um website institucional com áreas para acesso aos usuários e atores da rede, como portais de estudantes e professores, entre outras funcionalidades. Tais páginas web deverão se adequar à LGPD se coletarem e tratarem dados pessoais. Para tanto, a seguir, apresentamos um modelo de Política de Privacidade aplicável ao setor de educação, para fins meramente ilustrativos (ressaltando a necessidade de validar a redação da Política de Privacidade a ser adotada junto à respectiva assessoria jurídica competente, especialmente para verificar a sua adequação às particularidades das secretarias):

Política de Privacidade

Atualizado em @@.@@.@@@@

A presente Política de Privacidade ("Política de Privacidade") apresenta informações sobre a coleta, o acesso e o tratamento dos dados pessoais que você ("Usuário") [Nota: Fazer uma breve descrição sobre quem serão os usuários dos Serviços disponibilizados na Plataforma (ex.: apenas alunos, alunas e professores, professores e gestores, etc.)] disponibiliza à [QUALIFICAÇÃO DA **SECRETARIA DE EDUCAÇÃO**] (neste instrumento denominada "**SECRETARIA DE EDUCAÇÃO**") para os fins de utilização dos produtos, ferramentas e serviços educacionais ("Serviços") disponibilizados aos Usuários pela **SECRETARIA DE EDUCAÇÃO** por meio de sua plataforma disponível no Website <xxxxx> ("Plataforma").

A utilização dos Serviços importa imediata aceitação desta Política de Privacidade, bem como dos Termos de Uso. Ao acessar a Plataforma, você manifesta estar ciente desta Política de Privacidade que rege a sua relação com a **SECRETARIA DE EDUCAÇÃO**.

I. COLETA DE DADOS PESSOAIS

1.1. Para fins desta Política de Privacidade e à luz da legislação aplicável, a **SECRETARIA DE EDUCAÇÃO** entende como dado pessoal qualquer informação que identifique o Usuário ou permita a sua identificação. Por outro lado, dados anonimizados ou agregados não são considerados dados pessoais.

1.2. Todos os dados solicitados pela **SECRETARIA DE EDUCAÇÃO**

estão relacionados com os Serviços de educação pública prestados e são utilizados para aperfeiçoar estes Serviços, a experiência do Usuário na Plataforma da **SECRETARIA DE EDUCAÇÃO** e o desenvolvimento de novos Serviços que sejam do seu interesse.

1.3. Quando os Usuários visitam a Plataforma e utilizam os Serviços, nós coletamos dados pessoais desses Usuários, que incluem, mas não se limitam a:

1.3.1. **Dados cadastrais:** dados como nome, sobrenome, e-mail, endereço, cidade de residência e profissão, telefone de contato, RG, CPF, data de nascimento, gênero, dentre outros. Além disso, informações de sua conta, como usuário e senha, caso você tenha optado por criar uma conta em nossa Plataforma. [Nota: Adaptar a lista de dados de acordo com os que são efetivamente coletados pela **Secretaria de Educação**]

1.3.2. **Dados de estudantes:** dados como identidade, histórico escolar, informações médicas, endereço, telefone, e-mail, carteira estudantil, registro de aluno/a (RA), Número de Identificação Social (NIS), informações sobre necessidades especiais, bem como informações geradas durante o uso de tecnologias e que permitam identificar os alunos e alunas, como a gravação de imagens por câmeras de segurança, as análises geradas pelo uso de aplicativos educacionais, a coleta do IP do dispositivo móvel utilizado. [Nota: Adaptar a lista de dados de acordo com os que são efetivamente coletados pela **Secretaria de Educação**]

1.3.3. **Dados de docentes e demais servidoras e servidores públicos:** dados como identidade, idade, profissão, currículo, avaliação de desempenho, endereço, telefone, e-mail, salário, bem como informações geradas no uso de tecnologias e que permitam identificar essas pessoas, como a gravação de imagens por câmeras de segurança ou videoaulas, as análises geradas pelo uso de aplicativos educacionais, a coleta do IP do dispositivo móvel utilizado. [Nota: Adaptar a lista de dados de acordo com os que são efetivamente coletados pela **Secretaria de Educação**]

1.3.4. **Dados relacionados à navegação:** ao acessar a Plataforma da **SECRETARIA DE EDUCAÇÃO**, certas informações sobre o Usuário, como o protocolo de Internet (endereço IP), sistema operacional, tempo gasto na Plataforma, dentre outras informações serão armazenadas pela **SECRETARIA DE EDUCAÇÃO** ou por empresa contratada para essa finalidade. Caso não deseje fornecer esses dados, o Usuário poderá configurar o seu navegador de Internet ou o seu aparelho celular para desabilitar cookies, ficando ciente de que, nessa hipótese, a desativação de cookies poderá proporcionar um funcionamento limitado ou inadequado das funcionalidades da Plataforma da **SECRETARIA DE EDUCAÇÃO**. [Nota: Adaptar a lista de dados de acordo com os que são efetivamente coletados pela **Secretaria de Educação**]

1.3.5. **Dados adicionais:** na forma e nos limites do consentimento correspondente concedido pelo Usuário no uso dos Serviços (quando necessário), de

acordo com as disposições desta Política de Privacidade e dos Termos de Uso, e no limite do que for permitido pela lei. [Nota: Adaptar a lista de dados de acordo com os que são efetivamente coletados pela **Secretaria de Educação**]

1.4. A **SECRETARIA DE EDUCAÇÃO** coleta os dados pessoais dos Usuários das seguintes formas: (i) quando o Usuário cria uma conta ou perfil na Plataforma; (ii) informações enviadas por órgãos públicos, nas hipóteses previstas em lei; (iii) informações obtidas em razão do uso que é feito pelos Usuários da Plataforma da **SECRETARIA DE EDUCAÇÃO**; (iv) informações obtidas por meio de consulta a fontes e bancos de dados públicos; e (v) dados obtidos através de terceiros, por conta de parcerias estabelecidas para viabilizar o desenvolvimento de determinados Serviços da **SECRETARIA DE EDUCAÇÃO**. [Nota: Essa lista é meramente exemplificativa e deve ser adaptada à luz do caso concreto]

1.5. Em razão da prestação dos Serviços, a **SECRETARIA DE EDUCAÇÃO** coleta e realiza o tratamento de dados pessoais de menores de idade. Nessa hipótese, o tratamento de dados pessoais é sempre realizado no melhor interesse dos menores de idade, nos termos da legislação aplicável.

II. TRATAMENTO DE DADOS PESSOAIS

2.1. A **SECRETARIA DE EDUCAÇÃO** preza pela privacidade de seus Usuários e utiliza os dados pessoais coletados com as seguintes finalidades: [Nota: A lista a seguir é meramente exemplificativa e deve ser adaptada à luz das finalidades dos tratamentos realizados no caso concreto]

2.1.1. Executar os Serviços disponibilizados aos Usuários pela **SECRETARIA DE EDUCAÇÃO** por meio da Plataforma. Para cumprir essa finalidade, os dados pessoais poderão ser compartilhados com parceiros, nos moldes descritos na presente Política de Privacidade;

2.1.2. Permitir a comunicação com o usuário durante o uso dos Serviços, como para entrar em contato com o Usuário a fim de confirmar as informações que tenham sido fornecidas, e solicitar o envio de informações que ainda estejam pendentes para que a **SECRETARIA DE EDUCAÇÃO** possa prestar adequadamente seus Serviços;

2.1.3. Desenvolver estudos sobre os interesses, comportamentos e demografia dos Usuários para fornecer e personalizar os Serviços da **SECRETARIA DE EDUCAÇÃO** e melhorar de maneira contínua a experiência de navegação dos seus Usuários na Plataforma;

2.1.4. Os dados também poderão ser utilizados na gestão e melhoria das funcionalidades da Plataforma, bem como para a customização dos Serviços ofertados e a realização de estatísticas e estudos.

[Nota: Complementar com as demais finalidades aplicáveis, se for o caso]

2.2. Para a execução dos Serviços, a **SECRETARIA DE EDUCAÇÃO** poderá realizar, sempre respeitando a legislação pertinente, a transferência de dados pessoais fornecidos pelos Usuários para os parceiros operacionais da **SECRETARIA DE EDUCAÇÃO**.

2.2.1. No exercício de suas atividades, a **SECRETARIA DE EDUCAÇÃO** compartilha dados pessoais com terceiros, sempre com vistas a possibilitar e a aprimorar a oferta de seus Serviços, nos seguintes casos: (i) auxiliar no oferecimento ou na operação dos Serviços, através do compartilhamento de dados pessoais com prestadores de serviços e/ou parceiros, sempre dentro dos estritos limites autorizados pela legislação; (ii) analisar e solucionar problemas técnicos e relacionados a fraude e segurança da Plataforma e dos Serviços da **SECRETARIA DE EDUCAÇÃO**; (iii) cumprimento de obrigação legal, no sentido de que a **SECRETARIA DE EDUCAÇÃO** pode compartilhar dados pessoais conforme necessário para cumprir toda e qualquer determinação legal, seja ela judicial ou administrativa; e (iv) desenvolvimento de políticas públicas e prestação de serviços públicos, respeitados os princípios de proteção de dados pessoais. [Nota: Essa lista é meramente exemplificativa e deve ser adaptada à luz do caso concreto]

2.3. Além dos seus parceiros, a **SECRETARIA DE EDUCAÇÃO** não fornece os dados pessoais dos Usuários a terceiros fora de sua estrutura organizacional, salvo se necessário ao correto funcionamento da Plataforma, se houver autorização expressa do Usuário ou mediante ordem judicial e/ou outro procedimento previsto em Lei.

2.4. [Nota: Quando o armazenamento dos dados for feito no exterior] Os dados pessoais coletados poderão ser armazenados em servidores localizados no exterior - tendo em vista os serviços de armazenamento em nuvem que utilizamos - e somente serão fornecidos a terceiros na forma da Lei e/ou mediante ordem judicial.

2.5. Em todo o caso, os dados coletados por meio da Plataforma e em razão da execução dos Serviços disponibilizados serão armazenados apenas pelo período requerido pela respectiva regulamentação ou até o período necessário para atingir as finalidades para as quais foram coletados. Os dados serão então eliminados, na forma da lei, ressalvadas as seguintes hipóteses: (i) cumprimento de obrigação legal ou regulatória pela **SECRETARIA DE EDUCAÇÃO**; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; ou (iii) uso exclusivo da **SECRETARIA DE EDUCAÇÃO**, vedado o acesso por terceiro, e desde que anonimizados os dados.

III. DOS SISTEMAS E APLICATIVOS DE TERCEIROS

3.1. A Plataforma e os Serviços da **SECRETARIA DE EDUCAÇÃO** poderão conter *links* para produtos e serviços de terceiros, os quais possuem Políticas de Privacidade próprias. Esta Política de Privacidade se limita à Plataforma e aos Serviços oferecidos pela

SECRETARIA DE EDUCAÇÃO.

3.2. Caberá aos Usuários, antes de utilizar sistemas, aplicativos, sites e plataformas em geral de terceiros, ler atentamente sua respectiva Política de Privacidade, estando ciente que a **SECRETARIA DE EDUCAÇÃO** não possui qualquer responsabilidade ou ingerência sobre os tratamentos de dados pessoais eventualmente conduzidos por quaisquer terceiros.

IV. DOS DIREITOS E DEVERES DOS USUÁRIOS

4.1. Os Usuários garantem que os dados fornecidos são verdadeiros e atuais, comprometendo-se a atualizá-los sempre que houver qualquer modificação neles.

4.2. A **SECRETARIA DE EDUCAÇÃO** adotará medidas técnicas e organizacionais apropriadas para cumprir as suas obrigações em relação aos direitos dos Usuários enquanto titulares dos dados pessoais. Nesse sentido, a **SECRETARIA DE EDUCAÇÃO** se compromete a viabilizar da melhor forma possível os direitos dos Usuários, quais sejam:

4.2.1. **Confirmação**: direito a ser informado sobre a existência de tratamento.

4.2.2. **Acesso**: direito de solicitar o acesso aos dados pessoais tratados pela **SECRETARIA DE EDUCAÇÃO**.

4.2.3. **Correção**: direito de solicitar a alteração dos dados pessoais tratados pela **SECRETARIA DE EDUCAÇÃO** sempre que estiverem incompletos, inexatos ou desatualizados.

4.2.4. **Restrição**: direito de solicitar a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados pela **SECRETARIA DE EDUCAÇÃO** em desconformidade com a legislação de proteção de dados pessoais.

4.2.5. **Portabilidade**: direito de solicitar a transmissão dos dados tratados pela **SECRETARIA DE EDUCAÇÃO** para outro fornecedor de serviços.

4.2.6. **Eliminação**: direito de solicitar a eliminação dos dados pessoais tratados pela **SECRETARIA DE EDUCAÇÃO** com o consentimento do Usuário.

4.2.7. **Informação**: direito de ser informado sobre as entidades públicas e privadas com as quais a **SECRETARIA DE EDUCAÇÃO** compartilhou dados, sobre a possibilidade de não fornecer consentimento e sobre as consequências desta negativa.

4.2.8. **Revogação do consentimento**: direito de revogar

o consentimento a qualquer momento, através de manifestação expressa, por procedimento gratuito e facilitado.

4.2.9. **Revisão às decisões automatizadas**: possibilidade de revisão de decisões tomadas pela **SECRETARIA DE EDUCAÇÃO** unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

4.3. O Usuário deve entrar em contato com a **SECRETARIA DE EDUCAÇÃO** por meio do e-mail indicado na seção "Disposições gerais" abaixo caso tenha interesse em exercer algum dos direitos e deveres elencados acima.

4.4. Em relação à solicitação de eliminação dos dados pessoais dos Usuários, a **SECRETARIA DE EDUCAÇÃO** cumprirá pedidos de exclusão de dados pessoais mediante solicitação ou diante de obrigações legais.

V. SEGURANÇA DAS INFORMAÇÕES

5.1. Ao tratar os dados pessoais dos Usuários, a **SECRETARIA DE EDUCAÇÃO** se esforçará para armazená-los e mantê-los protegidos em ambientes seguros e controlados, respeitando a legislação vigente.

5.2. Restringimos o acesso aos dados pessoais às pessoas que necessitem dessas informações para prestar o suporte necessário aos Usuários, ou garantir o melhor funcionamento dos Serviços e da Plataforma. [Nota: Adaptar conforme o caso]

VI. DISPOSIÇÕES GERAIS

6.1. Esta Política de Privacidade consiste na versão válida e eficaz das informações sobre o tratamento dos dados pessoais dos Usuários pela **SECRETARIA DE EDUCAÇÃO**. Essa versão é responsável por governar todas as relações entre você e a **SECRETARIA DE EDUCAÇÃO**, exceto quando forem utilizados serviços que possuem Políticas de Privacidade próprias, respeitados os direitos adquiridos, os atos jurídicos perfeitos e as coisas julgadas.

6.2. A **SECRETARIA DE EDUCAÇÃO** se reserva o direito de atualizar e modificar periodicamente quaisquer de seus documentos jurídicos, incluindo esta Política de Privacidade. Qualquer modificação nesta Política que acarrete impacto no consentimento previamente fornecido para os Usuários (quando necessário) será comunicada pela **SECRETARIA DE EDUCAÇÃO** com antecedência. No entanto, qualquer alteração feita por razões legais ou devido a novas funcionalidades de um Serviço entrará em vigor imediatamente.

6.3. As cláusulas desta Política de Privacidade seguirão vigentes a qualquer forma de terminação, ocorrida por qualquer motivo, de modo a continuar a produzir efeitos sobre as partes enquanto houver relações jurídicas subsequentes.

6.4. Caso queira exercer algum dos direitos previstos nesta Política de Privacidade, ou tenha qualquer dúvida sobre este documento e as práticas nele descritas, o Usuário deverá entrar em contato com o(a) encarregado(a) da **SECRETARIA DE EDUCAÇÃO**, através do e-mail [inserir e-mail], ou do telefone [inserir telefone].

6.5. O Usuário se obriga a manter atualizado em seu cadastro o seu endereço eletrônico, por meio do qual se farão as comunicações a ele dirigidas pela **SECRETARIA DE EDUCAÇÃO**.

6.6. **O USUÁRIO RECONHECE QUE AS PECULIARIDADES SOBRE A COLETA, A UTILIZAÇÃO E O COMPARTILHAMENTO DE DADOS DA SECRETARIA DE EDUCAÇÃO FORAM SUFICIENTEMENTE DESCRITAS NESTA POLÍTICA E QUE A SECRETARIA DE EDUCAÇÃO CUMPRIU DEVIDAMENTE O SEU DEVER DE INFORMAÇÃO.**

6.7. **APÓS LER ATENTAMENTE ESTA POLÍTICA DE PRIVACIDADE, O USUÁRIO DECLARA ESTAR DE ACORDO COM ESTA POLÍTICA E ACEITA TODAS AS SUAS DISPOSIÇÕES.**

Anexo III – Modelo de termos de uso

Os Termos de Uso, por sua vez, representam um documento com informações sobre a interação entre a secretaria e o usuário ou usuária, a partir da descrição dos serviços disponibilizados no seu site ou plataforma, e das condições estabelecidas para o seu uso, como aquelas relacionadas a cadastro, obrigações, responsabilidades, direitos de propriedade intelectual e canais de comunicação. Tal qual a Política de Privacidade, os Termos de Uso devem ser disponibilizados de forma pública, em local de fácil acesso (ex.: no rodapé do seu website).

Vale ressaltar que os Termos de Uso e a Política de Privacidade são documentos distintos: enquanto os Termos de Uso buscam indicar a maneira pela qual os serviços são prestados, a Política de Privacidade possui enfoque na maneira pela qual são realizadas as atividades de tratamento de dados pessoais relacionadas a esses serviços. Por essa razão, é comum que esses documentos façam referência um ao outro (conforme indicado nos modelos disponibilizados neste Manual), e atuem de modo complementar a fim de fornecer informações mais claras e detalhadas aos usuários e usuárias a respeito das atividades em que estão envolvidos.

A seguir, apresentamos um modelo de Termos de Uso aplicável a serviços de educação fornecidos por órgãos ou entidades públicas, para fins meramente ilustrativos. Considerando a existência de websites institucionais de secretarias de educação estaduais e municipais com áreas para acesso aos usuários e atores da rede, como portais dos alunos e professores, entre outras funcionalidades, os Termos de Uso representam uma importante ferramenta para indicar com mais detalhes como ocorrerá a

relação entre website e usuários e usuárias, e fornecer informações relevantes para nortear o uso desses websites de maneira adequada. Nesse caso, ressaltamos mais uma vez a necessidade de validar a redação dos Termos de Uso a serem adotados junto à respectiva assessoria jurídica competente, especialmente para verificar a sua adequação às particularidades das secretarias e dos serviços oferecidos:

Termos de Uso

Atualizado em @@.@@.@@@@

Os Termos de Uso (“Termos de Uso” ou “Termos”) regem o relacionamento entre você (“Usuário”) [Nota: Fazer uma breve descrição sobre quem serão os usuários dos Serviços disponibilizados na Plataforma (ex.: apenas estudantes e familiares, estudantes, pais e professores, professores e gestores, etc.)] e a **QUALIFICAÇÃO DA SECRETARIA DE EDUCAÇÃO**] (doravante denominada “**SECRETARIA DE EDUCAÇÃO**”) para os fins de utilização dos produtos, ferramentas e serviços educacionais (“Serviços”) disponibilizados aos Usuários pela **SECRETARIA DE EDUCAÇÃO** por meio de plataforma disponível no Website <xxxxx> (“Plataforma”).

Estes Termos de Uso devem ser lidos em conjunto com a respectiva Política de Privacidade da **SECRETARIA DE EDUCAÇÃO** (“Política de Privacidade”). Os Termos de Uso e a Política de Privacidade (em conjunto, “Termos Gerais”) estabelecem os termos e condições aplicáveis ao uso da Plataforma pelos Usuários e aos Serviços prestados pela **SECRETARIA DE EDUCAÇÃO**.

A utilização dos Serviços, parcial ou integralmente, importa em imediata aceitação dos Termos Gerais. Assim, ao utilizar a Plataforma, você manifesta estar ciente destes Termos de Uso que regem a sua relação com a **SECRETARIA DE EDUCAÇÃO**.

I. DESCRIÇÃO E FINALIDADE DOS SERVIÇOS

1.1. Por meio de suas Plataformas, a **SECRETARIA DE EDUCAÇÃO** oferece gratuitamente um ecossistema gerador de soluções para que cada estudante alcance o seu pleno potencial de

aprendizagem e para que outros Usuários acessem produtos e serviços disponibilizados nas Plataformas, e que contempla os seguintes Serviços:

1.1.1. [Nota: Descrever os serviços que são oferecidos na Plataforma]
(...) *Exemplos de atividades: (i) Consulta aos Cadernos de Alunos; (ii) Acompanhamento de calendário escolar; (iii) lançamento de notas por professores; (iv) acesso a informações das unidades de ensino; (v) controle da lista de alunos das turmas; (vi) acompanhamento, por parte dos pais e responsáveis, das notas e frequência dos filhos; (vii) consulta ao boletim escolar; (viii) acesso ao histórico escolar dos alunos; (ix) elaboração de tarefas escolares.*

II. CADASTRO

2.1. Para acessar os Serviços, o Usuário precisará se cadastrar na Plataforma, informando obrigatoriamente alguns dados e fornecendo outros em caráter facultativo. O cadastro resultará na criação de um *login* e uma senha de acesso que identificam o Usuário na Plataforma. Os dados pessoais informados pelo Usuário, bem como os dados disponibilizados durante o uso dos Serviços, serão tratados em conformidade com o disposto na Política de Privacidade.

2.2. O Usuário é o único responsável pelo sigilo de sua senha, obrigando-se a mantê-la em segredo, devendo prontamente informar à **SECRETARIA DE EDUCAÇÃO**, nos termos do presente instrumento, qualquer indicação de uso indevido de seus *login* e senha por qualquer terceiro.

2.3. Ao se cadastrar, o Usuário se compromete a informar apenas dados verdadeiros e atualizados, sendo de sua exclusiva responsabilidade as consequências civis e penais advindas da prestação de informações incorretas ou falsas.

2.4. Em caso de dados falsos ou inexatos, a **SECRETARIA DE EDUCAÇÃO** se reserva o direito de não concluir o cadastramento ou bloquear as contas já existentes, impossibilitando o uso dos Serviços pelo Usuário, até que as informações sejam corrigidas.

2.5. Por meio da realização do cadastro, o Usuário declara e garante expressamente ser plenamente capaz, podendo exercer e usufruir livremente da Plataforma e dos Serviços.

> 2.5.1. As crianças deverão obter previamente a autorização expressa de um dos seus pais ou responsáveis legais para utilização da Plataforma e dos Serviços, sendo de responsabilidade exclusiva dos pais ou responsáveis legais a fiscalização das atividades e condutas dessas crianças, bem como a ciência e anuência em relação a estes Termos e o eventual acesso por menores sem a prévia autorização.

III. CONDIÇÕES DE ACESSO À PLATAFORMA E DE UTILIZAÇÃO DOS SERVIÇOS

3.1. Ao utilizar os Serviços oferecidos pela **SECRETARIA DE EDUCAÇÃO**, o Usuário expressa de imediato a sua aceitação, plena e sem reservas, dos Termos Gerais. Da mesma forma, o Usuário se compromete a observar e respeitar as leis e os contratos em vigor,

utilizando os Serviços apenas para fins lícitos e que respeitem quaisquer direitos de terceiros.

3.2. Os Serviços da **SECRETARIA DE EDUCAÇÃO** são voltados para o uso pessoal e não comercial do Usuário, e se destinam apenas a fins educacionais.

3.3. [Nota: quando houver a criação de canais de comunicação por parte da Secretaria de Educação] Através da aceitação dos Termos Gerais, o Usuário autoriza que a **SECRETARIA DE EDUCAÇÃO** crie canais de comunicação diretos ou indiretos com o Usuário, seja por e-mail, redes sociais, notificações de celular e outras modalidades.

3.4. [Nota: Cláusula a ser mantida para os casos em que for possível compartilhar informações decorrentes do uso dos Serviços em redes sociais como Facebook, Twitter, dentre outras] Alguns dos Serviços da **SECRETARIA DE EDUCAÇÃO** permitem que o Usuário compartilhe certas informações em redes sociais através dos seus perfis. Nesses casos, o Usuário se compromete a cumprir todos os termos e políticas das redes sociais aplicáveis, de modo que não cabe à **SECRETARIA DE EDUCAÇÃO** se responsabilizar por publicações feitas fora do ambiente dos seus Serviços.

3.5. Ao utilizar os Serviços, o Usuário se obriga a não praticar atos que possam danificar, inutilizar, sobrecarregar, deteriorar ou de qualquer forma modificar a Plataforma e o seu conteúdo conforme são disponibilizados.

3.6. É terminantemente vedado ao Usuário, ao acessar a Plataforma e utilizar os Serviços: (i) exibir, enviar ou de qualquer forma divulgar mensagens, arquivos, fotografias ou quaisquer dados ou materiais com conteúdo ilegal, violento, difamatório,

calunioso, sigiloso, abusivo, perigoso, degradante, pornográfico, discriminatório, racista ou de qualquer modo ilegais ou atentatórios à ordem pública; (ii) praticar ou fomentar a prática de quaisquer atos ou atividades ilegais; (iii) exibir, enviar ou de qualquer forma divulgar mensagens, arquivos, programas, rotinas ou *links* cujo recebimento possa não ser desejado pelo destinatário, tais como correntes, listas de distribuição, "*spamming*" e similares; e (iv) exibir, enviar ou de qualquer forma divulgar mensagens, arquivos, fotografias ou quaisquer dados ou materiais que violem direitos de propriedade intelectual ou qualquer outro direito.

3.7. A **SECRETARIA DE EDUCAÇÃO** poderá eliminar qualquer conteúdo relativo ao perfil do Usuário: (i) por determinação legal; (ii) em virtude de ordem judicial ou por determinação de autoridade competente; (iii) para evitar ou corrigir quaisquer elementos que, a seu exclusivo critério, possam trazer ou tenham trazido prejuízos ou qualquer tipo de dano à **SECRETARIA DE EDUCAÇÃO** ou a qualquer terceiro; (iv) para identificar, corrigir ou evitar quaisquer problemas técnicos na operação dos Serviços; e (v) quando tais conteúdos estiverem em desacordo com o previsto no presente instrumento ou na legislação aplicável.

3.8. O Usuário é o único responsável pela utilização que faz dos Serviços oferecidos pela **SECRETARIA DE EDUCAÇÃO**, isentando e obrigando-se a indenizar desde já a **SECRETARIA DE EDUCAÇÃO** ou qualquer terceiro por conta de eventuais danos advindos desse uso.

IV. SERVIÇOS DE TERCEIROS

4.1. Os Serviços da **SECRETARIA DE EDUCAÇÃO**, bem como sua Plataforma, podem integrar livremente aplicações de terceiros, com a finalidade de possibilitar à **SECRETARIA DE EDUCAÇÃO**

oferecer ou operar os Serviços. Esses serviços específicos são de responsabilidade dos terceiros que os disponibilizam, e serão regidos única e exclusivamente pelos termos de uso a eles aplicáveis, definidos por cada terceiro por eles responsáveis.

4.2. Nos casos em que a aceitação dos termos de uso de terceiros seja necessária para a utilização de determinados Serviços da **SECRETARIA DE EDUCAÇÃO**, a não aceitação destes termos pode limitar o acesso do Usuário aos Serviços.

4.3. A **SECRETARIA DE EDUCAÇÃO** não possui qualquer responsabilidade em relação a websites ou demais destinos de *links* que levem o Usuário para fora da Plataforma da **SECRETARIA DE EDUCAÇÃO**. Da mesma forma, a **SECRETARIA DE EDUCAÇÃO** não se responsabiliza por anúncios ou materiais de terceiros inseridos nos Serviços, nem pelos produtos e serviços eventualmente anunciados por terceiros.

V. PROPRIEDADE INTELECTUAL

5.1. Os presentes Termos de Uso concedem aos Usuários, por meio destes Termos e durante sua vigência, uma licença não exclusiva, não transferível, não sublicenciável e limitada, para acessar a Plataforma e fazer uso dos Serviços da **SECRETARIA DE EDUCAÇÃO**. Nem estes Termos de Uso nem o uso da Plataforma e dos Serviços transferem ou concedem ao Usuário quaisquer direitos, exceto pela licença limitada concedida acima.

5.2. As marcas, logotipos, nomes comerciais, layouts, gráficos e design de interface, imagens, ilustrações, fotografias, apresentações, vídeos, conteúdos escritos e de som e áudio, programas de computador, banco de dados, arquivos de transmissão

e quaisquer outras informações e direitos de propriedade intelectual da **SECRETARIA DE EDUCAÇÃO**, observados os termos das Leis nº 9.279/1996 (“Lei da Propriedade Industrial”), 9.609/1998 (“Lei do Software”) e 9.610/1998 (“Lei de Direitos Autorais”), e sem prejuízo das demais normas relativas à proteção da propriedade intelectual, estão devidamente reservados.

5.3. São vedados quaisquer atos ou contribuições tendentes a modificação das características, ampliação, alteração ou incorporação de quaisquer outros programas ou sistemas da **SECRETARIA DE EDUCAÇÃO**. Toda e qualquer forma de reprodução dos Serviços e da Plataforma, de forma gratuita ou onerosa, sob quaisquer modalidades, formas ou títulos é expressamente vedada.

5.4. O conteúdo disponibilizado na Plataforma e/ou acessado em razão do uso dos Serviços caracteriza somente autorização ao Usuário para uso não comercial, pessoal e intransferível, para visualizar os conteúdos presentes na Plataforma, não implicando qualquer licença, cessão ou transferência de titularidade de direitos da **SECRETARIA DE EDUCAÇÃO** ao Usuário relacionados ao conteúdo, marca ou outorga de demais direitos. Em caso de violação, a **SECRETARIA DE EDUCAÇÃO** se reserva o direito de determinar a imediata remoção do conteúdo, sem prejuízo de outras sanções cíveis e penais estabelecidas na legislação pertinente.

5.5. [Nota: Aplicável quando o Usuário puder criar conteúdos na Plataforma] Ao gerar qualquer conteúdo por meio e nos Serviços da **SECRETARIA DE EDUCAÇÃO**, o Usuário concede à **SECRETARIA DE EDUCAÇÃO** uma licença não exclusiva e não onerosa, sem limitação geográfica, passível de ser sublicenciada e transferida,

pelo prazo total de vigência da proteção dos direitos autorais definido pela legislação aplicável, no Brasil e no exterior, sobre todos os direitos autorais, direitos de marca e outros direitos de propriedade intelectual relacionados a qualquer conteúdo gerado por meio dos Serviços.

VI. DIRETRIZES E LIMITAÇÕES DE RESPONSABILIDADE

6.1. A **SECRETARIA DE EDUCAÇÃO** envidará esforços para que os Serviços e a Plataforma sejam plenamente acessíveis a todo e qualquer tempo. Todavia, não há garantia de que o acesso e a sua utilização ocorram sem qualquer falha ou de forma ininterrupta.

6.2. A **SECRETARIA DE EDUCAÇÃO** não tem obrigação de monitorar, fiscalizar ou controlar o uso que os Usuários fazem dos Serviços. Nesse sentido, a **SECRETARIA DE EDUCAÇÃO** não garante que os Usuários venham a utilizar a Plataforma em conformidade com os Termo Gerais, que governam o acesso da Plataforma e a utilização do Serviços, bem como com a legislação em vigor, tampouco se responsabiliza pelo conteúdo gerado pelo Usuário durante o uso dos Serviços.

6.3. A **SECRETARIA DE EDUCAÇÃO** envidará esforços para, dentro dos padrões recomendados de segurança, garantir que os dados pessoais informados pelos Usuários sejam protegidos e mantidos confidenciais. Todavia, a **SECRETARIA DE EDUCAÇÃO** não pode garantir que a proteção dos dados e sua segurança jamais venham a ser violados.

6.4. O Usuário é o único responsável por qualquer informação que vier a disponibilizar em razão da utilização dos Serviços e pelo uso que faz da Plataforma, respondendo integralmente por qualquer

ofensa a direitos de terceiros que sua atuação possa causar.

VII. DISPOSIÇÕES GERAIS

7.1. O presente documento consiste na versão válida e eficaz dos Termos de Uso. Essa versão é responsável por governar todas as relações entre o Usuário e a **SECRETARIA DE EDUCAÇÃO**, exceto quando o Usuário utilizar serviços que possuem termos ou regramentos próprios, respeitados os direitos adquiridos, os atos jurídicos perfeitos e as coisas julgadas.

7.2. **A SECRETARIA DE EDUCAÇÃO** se reserva o direito de atualizar e modificar periodicamente quaisquer de seus documentos jurídicos, incluindo estes Termos de Uso.

7.3. Caso qualquer disposição destes Termos seja considerada inválida ou inexequível, por qualquer motivo, o mesmo não ocorre em relação às disposições restantes.

7.4. Existindo dúvidas sobre este instrumento ou sobre o que ele engloba, o Usuário pode entrar em contato com a **SECRETARIA DE EDUCAÇÃO** através do e-mail **[x]**.

7.5. Estes Termos são regidos pelas leis da República Federativa do Brasil.

7.6. Fica eleito, desde já, o foro de **@@@** para dirimir eventuais controvérsias oriundas dos presentes Termos de Uso, renunciando expressamente a qualquer outro, por mais privilegiado que seja.

7.7. O USUÁRIO RECONHECE QUE AS PECULIARIDADES DE USO DOS SERVIÇOS DA SECRETARIA DE EDUCAÇÃO FORAM SUFICIENTEMENTE DESCRITAS NESTES TERMOS E QUE A SECRETARIA DE EDUCAÇÃO CUMPRIU DEVIDAMENTE O SEU DEVER DE INFORMAÇÃO.

7.8. O USUÁRIO DECLARA TER LIDO ATENTAMENTE E COMPREENDIDO OS TERMOS E DISPOSIÇÕES DESTES TERMOS DE USO, ESTAR CIENTE DE SEU INTEIRO TEOR, E ESTAR DE ACORDO COM ESTES TERMOS, ACEITANDO TODAS AS SUAS CONDIÇÕES.

EXPEDIENTE

Responsáveis pela elaboração do Manual:

RENNÓ PENTEADO SAMPAIO ADVOGADOS
PEREIRA NETO | MACEDO ADVOGADOS

Flávia Parra Cano
Leonardo Chain de Oliveira
Natalia Langenegger
Ronaldo Lemos
Sofia Lima Franco
Vinícius Padrão

CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA - CIEB

Diretora-presidente
Lúcia Dellagnelo

Gerente-executiva
Gabriela Gambi

Coordenador de Compras Públicas
Thalles Gomes

Analista Sênior de Comunicação
Marina Kuzuyabu

Analista Sênior de Compras Públicas e responsável pela publicação
Gabriel Romitelli

REPRESENTAÇÃO DA UNESCO NO BRASIL

Diretora e Representante
Marlova Jovchelovitch Noleto

Coordenador do Setor de Comunicação e Informação
Adauto Cândido Soares

CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

Cooperação Representação no Brasil

APOIO

FUNDAÇÃO Lemann

imaginable futures