



Guia de tratamento de dados pessoais para servidores da UNICAMP

VERSÃO 1.0 | AGO. 2023



ESCRITÓRIO DE
PROTEÇÃO DE
DADOS PESSOAIS

Guia de tratamento
de dados pessoais para
servidores da UNICAMP

VERSÃO 1.0 | AGO. 2023

Mensagem do DPO

(Data Protection Officer - Encarregado de Tratamento de Dados Pessoais)

Os dados pessoais que compartilhamos com diversas entidades diariamente têm grande valor para nós e para a sociedade. Para as inúmeras atividades do nosso cotidiano, compartilhamos dados como: CPF, endereço e telefone. No mundo virtual, compartilhamos informações pessoais para fazer compras e para usar as redes sociais.

Para garantir que seus dados pessoais sejam utilizados de forma adequada e os seus direitos sejam preservados, foi aprovada a Lei Geral de Proteção de Dados Pessoais – LGPD.

A LGPD permite e regula a coleta e o tratamento de dados pessoais por empresas e órgãos públicos, além de definir regras e punições, em caso de utilização inadequada de dados pessoais.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, criou normas para o tratamento de dados pessoais, por empresas e órgãos públicos, com o objetivo de proteger os dados pessoais dos cidadãos, garantindo-lhes os direitos de liberdade, de privacidade e o livre desenvolvimento da personalidade.

Assim, por meio da LGPD, o cidadão pode controlar os seus dados pessoais e exercer os seus direitos, previstos na Lei.

A Unicamp tem demonstrado a sua preocupação em garantir a privacidade dos titulares dos dados pessoais sob a sua guarda. Porém, você também precisa estar atento com os seus dados pessoais, evitando fornecê-los sem necessidade, observando sempre a finalidade justificada para a qual seus dados serão tratados.

Este Guia foi pensado para orientar as atividades dos servidores que atuam na Universidade. Através de uma linguagem acessível e intuitiva, o objetivo é conduzir o servidor sempre pelos caminhos do pensar a LGPD durante a execução de suas atividades cotidianas.

Boa Leitura!

IDENTIFICAÇÃO DO CONTROLADOR

O Controlador é a pessoa natural ou jurídica, de direito público ou privado, responsável pelo tratamento dos dados pessoais e quem define a hipótese legal, a finalidade e o modo como os dados serão tratados.

A Universidade Estadual de Campinas é uma Autarquia Estadual, de regime especial; Administração Pública Indireta do Estado de São Paulo, com autonomia didático-científica, administrativa e de gestão financeira, patrimonial e disciplinar.

Denominação: Universidade Estadual de Campinas – UNICAMP

CNPJ: 046068425/0001-33

Site institucional: <https://www.unicamp.br>

Endereço: Rua da Reitoria S/N, Cidade Universitária “Zeferino Vaz” Campinas/SP – Brasil

IDENTIFICAÇÃO DO ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS

O Encarregado, também conhecido como Oficial de Proteção de Dados é o responsável por orientar a comunidade universitária, sobre as práticas de tratamento de dados, no âmbito da Unicamp.

ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS

Prof. Dr. Ricardo Dahab
Diretor Geral de Tecnologia da Informação e Comunicação – TIC
Email: dpo@unicamp.br

ESCRITÓRIO DE PROTEÇÃO DE DADOS PESSOAIS – EPDP

Prof. Dr. Ricardo Dahab – Coordenação
Lindinalva Candido Machado – Assistente Técnica LGPD

PROJETO GRÁFICO E DIAGRAMAÇÃO

Giacko Studio

COLABORAÇÃO E REVISÃO

Tee Global
Empresa filha da Unicamp



**COMITÊ GESTOR DE PRIVACIDADE E PROTEÇÃO
DE DADOS PESSOAIS CGPPD/UNICAMP**

UNIDADE/ÓRGÃO MEMBRO

PRESIDENTE Prof. Dr. Ricardo Dahab

FCM/DEAS Prof. Dr. José Roberto
Matos Souza

FCM/CAISM Prof. Dr. João Renato
Bennini Junior

PRP Prof. Dr. Marcelo Brocchi

COMVEST Prof. Dr. Rafael
Pimentel Maia

CCUEC Profa. Dra. Islene
Calciolari Garcia

PG Dra. Livia Ribeiro
de Padua Duarte

CGU Silviane Duarte Rodrigues

CGU Alexandre Henrique
de Melo

SIARQ Janaína Andiará
dos Santos

DGA Danilo Jorge Zanetti

DAC Silvio de Souza

DGRH Thiago Ricardo Sbrici

SIC Fábio Rodrigo Pinheiro
da Silva

SBU Daniela Feijó Simões

UNIDADE/ÓRGÃO MEMBROS CONVIDADOS

IFCH Prof. Dr. Thiago Nicodemo

IOU Alessandra Nazareth
Caine P. Roscan

Sumário

| | | | | | |
|------|---|----|-------|--|----|
| I. | APRESENTAÇÃO | 12 | g. | Portabilidade | 25 |
| II. | CONSIDERAÇÕES INICIAIS | 13 | h. | Peticionamento | 26 |
| | a. Unicamp - Controlador de dados pessoais. | 13 | i. | Oposição | 26 |
| | b. Servidores Técnicos e Docentes | 14 | j. | Revisão de decisões | 26 |
| | c. A LGPD e outras Legislações Nacionais | 15 | VI. | MAPA DE TRATAMENTO DE DADOS PESSOAIS | 27 |
| | d. Territorialidade | 17 | VII. | HIPÓTESES DE TRATAMENTO – BASE LEGAL | 29 |
| III. | RELAÇÃO JURÍDICA | 18 | i. | Obrigação Legal | 29 |
| | a. Tratamento de dados pessoais | 19 | ii. | Interesse do Titular | 30 |
| IV. | PRINCÍPIOS | 21 | iii. | Políticas Públicas | 31 |
| | a. Finalidade | 21 | iv. | Consentimento | 31 |
| | b. Adequação | 21 | VIII. | TIPOS DE DADOS - METADADOS | 33 |
| | c. Necessidade | 22 | IX. | COMPARTILHAMENTO DE DADOS NA ROTINA ADMINISTRATIVA | 35 |
| | d. Não discriminação | 22 | a. | Requisitos para o compartilhamento | 36 |
| V. | DIREITO DOS TITULARES DOS DADOS PESSOAIS | 22 | b. | Compartilhamento por e-mail | 36 |
| | a. Informação | 24 | c. | Uso secundário de dados pessoais | 37 |
| | b. Acesso | 24 | d. | Divulgação pública de dados pessoais, por servidores | 38 |
| | c. Correção | 24 | X. | LGPD NA UNICAMP | 39 |
| | d. Anonimização | 24 | | | |
| | e. Eliminação | 25 | | | |
| | f. Bloqueio | 25 | | | |

Apresentação

O tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 – LGPD).

Diante desse cenário, o desafio é o de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais, realizadas por órgãos e entidades públicos. Trata-se de assegurar a **celeridade e a eficiência** necessárias à execução de políticas e à prestação de serviços públicos, com respeito aos direitos à proteção de dados pessoais e à privacidade.

Este Guia foi pensado para orientar as atividades dos servidores que atuam na Universidade. Através de uma linguagem acessível e intuitiva, o objetivo é conduzir o servidor sempre pelos caminhos do pensar a LGPD durante a execução de suas atividades cotidianas.

A proposta desse Guia é oferecer conceitos úteis, extraídos da LGPD, organizados de tal modo, que o servidor possa sempre obter uma resposta e um caminho, quando o assunto for a privacidade e a proteção de dados pessoais sob a guarda da Universidade.

Considerações iniciais

UNICAMP – CONTROLADOR DE DADOS PESSOAIS

A Universidade é uma autarquia, autônoma em política educacional, subsidiada majoritariamente pelo governo do estado de São Paulo. Essa condição lhe atribui personalidade jurídica própria para o exercício de suas atividades administrativas, cuja autonomia deve ser guiada pelas prerrogativas do interesse público.

Assim, a Unicamp é responsável pelas iniciativas de adequação à Lei Geral de Proteção de Dados Pessoais, na condição de CONTROLADORA DE DADOS PESSOAIS, o que lhe impõe a missão de fornecer **informações claras e precisas**, sobre a finalidade específica do tratamento de dados pessoais dos titulares com os quais possui vínculo.

Como parte desse novo rol de responsabilidades, trazido pela LGPD, a Universidade atenderá os direitos do titular e cumprirá todas as obrigações de tratamento de dados pessoais conforme as disposições legais.

Os servidores participam como parte integrante e ativa desse grande projeto de gestão, a partir da execução de medidas práticas no dia a dia, refletindo sempre sobre a privacidade dos titulares, no momento em que manuseiam seus dados pessoais.

SERVIDORES TÉCNICOS E DOCENTES

Os servidores técnicos e docentes são os destinatários principais da elaboração deste Guia.



São eles que atuarão, em nome da Universidade, executando as diretrizes da LGPD. Resta saber portanto, qual o seu grau de responsabilidade pessoal na aplicação da proteção de dados nas atividades do cotidiano.

Segundo uma recente interpretação da Autoridade Nacional de Proteção de Dados Pessoais, ANPD, “não são considerados controladores ou operadores **os indivíduos subordinados**, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam dentro da estrutura organizacional do Controlador e, portanto, sob o seu poder diretivo”.

Isso significa que fora das estruturas da Universidade, o servidor não pode ser invocado pessoalmente a responder por questões

envolvendo à LGPD, mas poderá responder internamente perante a Universidade. Implica dizer também que as penalidades previstas na LGPD não podem ser aplicadas diretamente ao servidor.

É importante lembrar que as demais penalidades previstas na lei civil e regimentos do próprio exercício da função pública, continuam em vigor. Ou seja, podem ser aplicadas em caso de apuração infracional do servidor, independente do que diz a LGPD.

A LGPD E OUTRAS LEGISLAÇÕES NACIONAIS

A Constituição Federal, quando tratou dos direitos e garantias fundamentais, em 1988, estabeleceu a importância, em seu artigo 5º, da proteção da intimidade e a vida privada. A Lei de Acesso à Informação, LAI, em 2011, abordou pela primeira vez, expressamente, sobre a necessidade de tratar informações pessoais, respeitando a intimidade e a vida privada. O Marco Civil da Internet, Lei de 2014, fixou o conceito de ‘**proteção de dados pessoais**’ que mais tarde, em 2018, viria a ser o núcleo de atenção da própria LGPD.

A LGPD, portanto, foi concebida como uma norma unificadora de todos os conceitos e perspectivas que já estavam delineados em legislações anteriores. Seu objetivo principal é garantir **o direito do cidadão de exercer a gestão e o controle sobre o tratamento dos seus dados pessoais**.

Assim, a LGPD deve ser sempre interpretada de modo a complementar a aplicação de outras

normas, não excluindo conceitos que já foram consolidados em disposições anteriores.



Sobre o aparente conflito de normas que poderia existir entre a LGPD e a Lei de Acesso à Informação, por exemplo, no que diz respeito à exibição dos salários e nomes dos servidores públicos, até o presente momento, aplica-se a interpretação do PARECER n. 00001/2021/CONJUR-CGU/CGU/AGU, p. 18, item 22 e seguintes.

Conforme decidido pelo STF, “a remuneração dos agentes públicos constitui informação de interesse coletivo ou geral”, aplicando-se à hipótese o princípio constitucional da publicidade administrativa, que “propicia o controle da atividade estatal até mesmo pelos cidadãos.” A Corte entendeu, ainda, que os riscos pessoais decorrentes da divulgação são atenuados com “a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor”. Por fim, em atenção ao contexto e às expectativas dos titulares envolvidos, a decisão menciona que “os dados, objeto de divulgação em

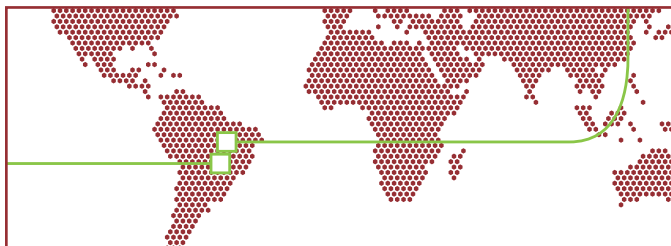
causa, dizem respeito a agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo nessa qualidade”.

TERRITORIALIDADE

A LGPD é aplicável para todas as pessoas físicas e jurídicas que tratam dados pessoais de terceiros **dentro do território brasileiro**. Não importa a nacionalidade do titular de dados. A lei se aplica para todo tratamento de dados realizado em território nacional.

Isso ajuda a pensar a LGPD quando envolve uma pesquisa com dados pessoais localizados em ambientes internacionais. Todas as vezes que dados pessoais forem transferidos desses ambientes, para uma finalidade vinculada a uma coleta/pesquisa, é importante aplicar os conceitos da LGPD, independente do cuidado que se tenha dado a esses dados no ambiente internacional, onde a informação foi obtida.

Dois pontos devem ser considerados ao importar dados pessoais de terceiros, de ambientes internacionais para o ambiente da Universidade: (1) certifique-se sempre se houve autorização específica dos titulares para aquela divulgação dos seus dados; (2) ou, se os dados estão anonimizados, protegendo assim, a identificação do titular. Se nenhuma dessas informações puder ser deduzida do que consta na plataforma, procure um contato do DPO (*data protection officer* – encarregado de dados pessoais) e solicite essa informação.



Lembre-se que, quando você gera uma evidência de que se esforçou para obter a informação que protegerá o titular de dados pessoais, você contribuiu para a mitigação de riscos envolvendo a privacidade de terceiros e com isso, também protege a sua atuação enquanto servidor e a própria Universidade.

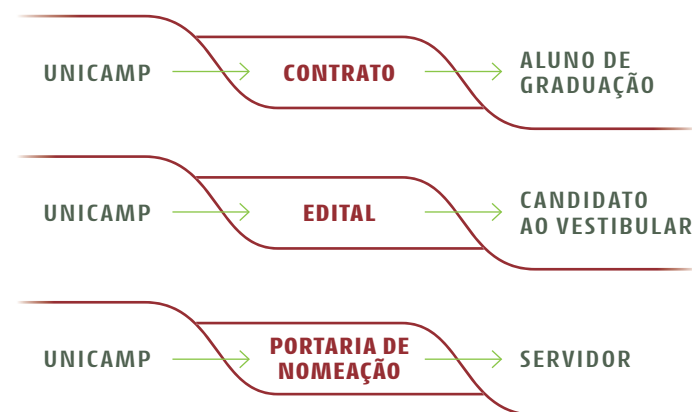
Gerar evidências de que você coloca a LGPD em prática é fundamental para a efetiva proteção de dados pessoais exigida pela nova lei.

Relação Jurídica

A relação jurídica que você precisa observar para aplicar a LGPD é aquela existente entre a Universidade e o titular de dados que confiou suas informações pessoais, para a execução de uma (ou algumas) finalidade específicas e informadas previamente a esse titular.

Você, enquanto servidor, é um representante ativo da Universidade dentro dessa relação jurídica.

Dizemos que esta é sempre uma relação **jurídica** porque depende de um contrato, um acordo, um vínculo entre as partes. E nesse documento, constam os direitos e obrigações assumidos por ambas as partes.



TRATAMENTO DE DADOS PESSOAIS

Tratar dados na atividade cotidiana do servidor, e segundo a perspectiva da LGPD, significa garantir que:

- o uso desses dados esteja vinculado a uma finalidade;
- existe uma base legal que permite esse tratamento;
- os locais de armazenamento e os sistemas envolvidos, na teia de compartilhamento

dessa informação, foram divulgados para conhecimento do titular de dados;

- há um prazo de retenção dessas informações, uma vez que o seu uso não pode ser por prazo injustificado.

Para se manter dentro da trilha do tratamento adequado de dados pessoais, o servidor poderá recorrer a três pilares fundamentais:

SEGURANÇA

Você só pode tratar dados para determinada finalidade se essa finalidade for compatível com as atribuições da função para a qual você foi nomeado.

PREVISIBILIDADE

A finalidade de tratamento de dados pessoais deve estar fundamentada em uma das bases legais fixadas na LGPD.

TRANSPARÊNCIA

A finalidade de tratamento deve ter sido informada ao titular de dados (essa informação constará sempre no contrato/ vínculo que une a Universidade e o titular de dados.

Princípios

O artigo 6º da LGPD fixa os princípios que devem ser observados para um tratamento adequado de dados pessoais. De todos os princípios, alguns precisam ser lembrados pelo servidor durante o exercício da sua função, quando isso envolver o manuseio de dados pessoais. Outros princípios já são observados pela própria Universidade, pois envolvem medidas técnicas estruturais.

Aqui vamos falar somente daqueles que implicam diretamente a sua atividade.

Sobre os princípios que precisam ser observados pelo servidor:

FINALIDADE

O tratamento de dados pessoais, do qual você participa no exercício das suas funções, deve estar vinculado a uma ou mais finalidades. Para saber sobre a ocasião do tratamento de dados, entenda o que consta no ‘acordo’ existente entre a Universidade e o titular de dados.

ADEQUAÇÃO

A finalidade para a qual os dados pessoais estão sendo tratados deve ter sido informada aos titulares. Tratamento adequado de dados é sempre aquele que foi informado antes de acontecer.

NECESSIDADE

Os dados acessados para a realização da finalidade devem ser, somente, aqueles estritamente necessários para atingir a finalidade. Faça uma revisão dos processos que envolvem o tratamento de dados pessoais e comunique à Universidade, caso você entenda que pode haver uso excessivo ou injustificado de dados pessoais.

NÃO DISCRIMINAÇÃO

Quando você estiver tratando dados pessoais, garanta que não haja divulgação ou compartilhamento que venha a causar algum tipo de constrangimento ao titular. Por exemplo, a divulgação de notas dos alunos no pátio, através da fixação de planilhas no quadro. Evite colocar o nome do aluno associado à nota. Escolha colocar o número de matrícula. Isso será interpretado como uma medida de mitigação de riscos, uma vez que o número da matrícula configura um processo de anonimização parcial, protegendo a identificação imediata do aluno.

Direito dos titulares dos dados pessoais

O titular de dados pessoais pode reivindicar e requerer ações referentes aos direitos que a LGPD lhe especifica. Caso você seja abordado por algum titular de dados que queira fazer algum tipo de requisição, procure se informar sobre o ‘canal de requisições’ que a Universidade coloca à disposição para esse tipo de ocorrência.



Prefira sempre encaminhar o titular para esse ‘canal de requisições’ evitando que essa abordagem aconteça com você diretamente. Isso porque o mais adequado, sempre, é que um encarregado de dados pessoais responda qualquer tipo de requisição envolvendo dados pessoais. No final do guia, informamos os endereços eletrônicos que podem levar você até o ‘canal de requisições’ ou contato do encarregado de dados.

Sobre todos os direitos dos titulares de dados, a relação é fixada pela LGPD no Capítulo III, artigo 17 e seguintes. São direitos de todo titular de dados pessoais:

INFORMAÇÃO

Fornecer aos titulares, informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais.

ACESSO

Obter informações sobre quais dados pessoais a Universidade está coletando e como estão sendo utilizados.

CORREÇÃO

Obter a correção de dados imprecisos, incompletos ou desatualizados que a Universidade possua sobre eles.

ANONIMIZAÇÃO



Ter os dados anonimizados evitando a exposição da identificação do titular. A Universidade sempre que possível utilizará recursos de anonimização total ou parcial, para evitar a exposição desnecessária da identidade dos titulares. Mas ainda assim, se o titular entender que foi exposto de alguma forma não compatível com a sua privacidade, ele pode requerer a anonimização.

A Universidade atenderá essa requisição sempre que a omissão da identificação do titular não comprometer a realização do tratamento de dados.

ELIMINAÇÃO

É o direito ao esquecimento. Consiste no encerramento total das operações de tratamento e o consequente descarte dos dados pessoais. Quando eliminados, os dados não podem ser reutilizados para nenhum tipo de tratamento. Isso só será possível desde que não haja nenhuma disposição legal que obrigue o Controlador à retenção desses dados por mais tempo.

BLOQUEIO

Ter o uso dos dados pessoais, pela Universidade, suspenso temporariamente.

PORTABILIDADE



Receber seus dados pessoais em formato estruturado, possibilitando a transferência para outro serviço ou

empresa, a pedido do titular. O direito à portabilidade pressupõe que a própria Universidade é quem fará a transferência dos dados estruturados para o outro Controlador, indicado pelo titular no seu requerimento. Esse direito depende de pronunciamento através de decreto regulador.

PETICIONAMENTO

Deixar disponível um ambiente em que todo titular de dados pessoais, vinculado à Universidade, possa protocolar petições e requerimentos relacionados aos seus dados pessoais.

OPOSIÇÃO

Os titulares podem se opor ao tratamento de seus dados, cabendo à Universidade, através do contato com o DPO, responder justificadamente sobre a oposição requerida.

REVISÃO DE DECISÕES

Os titulares têm o direito de solicitar a revisão de **decisões automatizadas**.

Decisão automatizada é aquela que ocorre no banco de dados da Universidade, mas que não necessariamente, tenha sido comunicada pontualmente ao titular. Por exemplo, uma pesquisa interna em que, com base no número de matrículas, algum departamento precise saber ‘quantos alunos de graduação tem mais de 60 anos’.

Não há nenhum problema na tomada desse tipo de decisão automatizada pela Universidade, cabendo apenas o cuidado de entender se as decisões automatizadas estão fundamentadas pelo **legítimo interesse**, ou seja quando for necessário para o cumprimento e atribuições da Universidade. Outro cuidado que precisa estar presente no momento de uma decisão automatizada é que esta será possível, desde que não viole os direitos e as liberdades fundamentais do titular.

Mapa de tratamento de dados pessoais

A seguir, apresentamos o mapa de tratamento de dados pessoais. Sempre que o servidor precisar pensar sobre a LGPD no exercício de suas atividades funcionais, sugerimos que seja preenchido o mapa, para entender se a sua atividade, ao envolver o tratamento de dados pessoais, está dentro de um contexto possível, legal e compatível com a sua atividade funcional. Mantendo-se dentro desses limites de atuação, o servidor sempre estará agindo em conformidade com a proteção de dados pessoais.

| MAPA DE TRATAMENTO DE DADOS | |
|--|-------------------------|
| (Vínculo entre a universidade e o titular de dados) | Finalidade |
| (O que você faz para contribuir com a realização da finalidade? Isso está inserido dentro da competência para a qual você foi nomeado? (cargo/função)) | Motivo da coleta |
| (Qual a base legal que fundamenta o tratamento de dados pessoais que você realiza?) | Base legal |
| Onde você acessa os dados pessoais que manuseia? (sistemas/pastas/fornecedores terceirizados) Para onde você remete esses dados após o tratamento? | Compartilhamento |
| Qual a classe de titulares? (alunos, pacientes, servidores técnicos, servidores docentes) | Titular |
| Qua(is) o(s) tipo(s) de dado(s)? (nome, data de nascimento, rg, cpf, cnh) | Metadados |

HIPÓTESES DE TRATAMENTO – BASE LEGAL

Tratar dados pessoais de terceiros significa manusear essas informações, para a realização de uma finalidade lícita e informada ao proprietário desses dados.

Todo tratamento de dados pessoais precisa se enquadrar em uma hipótese de tratamento definida no art. 7º da LGPD. De todas as hipóteses previstas na lei, vamos falar sobre aquelas que fazem sentido na aplicação da proteção de dados nas rotinas administrativas e nas atividades docentes da Universidade.

OBRIGAÇÃO LEGAL

Quando o tratamento de dados é necessário para cumprir uma obrigação legal ou regulatória a qual a Universidade está submetida.



É o que fazem os servidores que atuam nas atividades de recursos humanos, quando enviam informações pessoais para preenchimento de declarações necessárias à previdência social (ou estatutária) e ao informe de rendimentos.

Outro exemplo é quando a Universidade arquiva dados do aluno para além do tempo em que ele

esteve matriculado; ou arquiva dados dos seus servidores, em razão de algum regulamento legal.

Sempre haverá uma lei, um decreto, um ato normativo (de qualquer hierarquia), por trás dessa hipótese legal, que existe para o cumprimento de uma obrigação.

Assim, se você manuseia dados pessoais com base em alguma determinação fixada por outra lei, essa hipótese de tratamento é legítima.

INTERESSE DO TITULAR

Quando o tratamento de dados é realizado para atender um interesse manifestado pelo próprio titular de dados.

Quando um candidato se inscreve para uma seleção de vaga, em edital publicado pela Universidade, naquele momento ele está concordando com as regras daquela seleção, dentre elas, o oferecimento dos seus dados para que ele possa participar do processo seletivo.

Quando o candidato se torna um aluno, outras informações são coletadas para o registro de matrícula. Nesse caso, mais uma vez, o titular entrega seus dados para que ele seja matriculado.

Em outros casos, os titulares de dados tem interesse em serviços pontuais que a Universidade oferece, como empréstimo de livros para usuários externos, eventos educacionais e culturais passíveis de inscrição e certificado de participação.

Sempre que o titular dos dados manifestar interesse na realização de um serviço/um cargo/uma

bolsa, oferecidos pela Universidade, a hipótese legal que fundamentará o tratamento de dados pessoais (por você, servidor), será aquela estabelecida no art. 7º, inciso V: “V - *quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados*”.

POLÍTICAS PÚBLICAS

Esta hipótese de tratamento de dados pessoais ocorre quando o manuseio de dados, pelo servidor, se justifica pela existência de uma Política Pública formalmente instituída. Caso você fique em dúvida, se a hipótese de tratamento é uma **política pública** ou o cumprimento de uma **obrigação legal**, lembre-se de que, quando for o caso de uma política pública, a lei que a instituiu terá o nome: ‘Política Pública Xxxxxx, Programa Xxxxxx’, como nesse exemplo: *Programa “4004 - Transparência, Integridade e Combate à Corrupção - Objetivo 1213 - Fortalecer a Governança, a Gestão, a Transparência, a Participação Social e o Combate à Corrupção “*

CONSENTIMENTO

Não é por acaso que colocamos essa hipótese de tratamento por último. Serão pontuais os casos em que um servidor precisará tomar o consentimento pessoal do titular de dados, para executar uma finalidade de tratamento.

Na maioria dos casos, o servidor atua para a consecução das atividades em nome da Universidade,

que por sua vez, já estabeleceu com o titular de dados algum acordo sobre a performance do tratamento de dados pessoais. Ou seja, o servidor não terá o desafio de intuir se precisa tomar a iniciativa de colher o consentimento do titular por sua conta, antes de executar o tratamento.

Quando for o caso dessa hipótese de tratamento ser adotada para justificar o manuseio de dados, essa será uma determinação dirigida expressa e diretamente ao servidor, pela autoridade institucional responsável pela Privacidade de Dados Pessoais dentro da Universidade.



Pela hipótese legal do Consentimento, o tratamento de dados só pode ser realizado com a evidência de que o titular autorizou. Uma hipótese que podemos constatar na coleta de dados pessoais para pesquisas acadêmicas, quando a identidade do entrevistado (alguém externo) não puder ser anonimizada.

Outra situação, é quando o titular se inscreve em um evento da Universidade e, por ocasião dessa inscrição são enviados emails divulgando outros eventos futuros. Esse contato para divulgação de novos eventos só poderá acontecer se o titular autorizar.

Tipos de dados - Metadados

Definir os tipos de dados, que estão sendo utilizados, para atingir determinada finalidade de tratamento é fundamental em um cenário de vivência da LGPD.

Isso porque um dos Princípios que a lei exige que sejam observados, é o da Necessidade. Só podem ser utilizados, em uma atividade de tratamento de dados, aquelas informações minimamente necessárias para a execução da finalidade pré definida. O objetivo disso é evitar a coleta ou acesso a uma qualidade de dados excessiva, o que seria prejudicial para a Universidade.

Os tipos de dados utilizados precisam ser compatíveis com a finalidade do tratamento e com o rol de competências funcionais do servidor.

Se um dado de saúde for coletado para um processo seletivo, isso precisa ser justificado, ter uma função prática dentro do processo de seleção.

A data de nascimento de uma aluno, não precisa constar em um painel para a divulgação de notas finais de prova (por exemplo). O número de matrícula pode bastar.

Assim, tomar conhecimento dos tipos de dados utilizados para atingir determinada finalidade é necessário para que o servidor esteja seguro quanto à legitimidade desse acesso.

Existem vários tipos de dados: cadastrais, de saúde, menores de idade, financeiros, bancários, sócio econômicos, dentre outros. Cada tipo de dado contém um rol do que chamamos de METADADOS¹.

¹ Metadados, são dados sobre outros dados. Os metadados facilitam o entendimento dos relacionamentos e a utilidade das informações dos dados.

DADO PESSOAL

(rg, cpf, data de nascimento, certidão de casamento, etc)

DADO PESSOAL SENSÍVEL

(tipo sanguíneo, sexo biológico, religião, partido político)

DADOS DE CRIANÇA E ADOLESCENTE

(dados gerais quando estes se referirem a pessoas menores de 21 anos e 12 anos)

DADO PÚBLICO

(dados pessoais que se tornaram públicos pela iniciativa do titular sem qualquer solicitação do Controlador)

DADO ANONIMIZADO OU PSEUDONIMIZADO

(dados pessoais cujo processo de anonimização total ou parcial impessa a identificação do titular)

Compartilhamento de dados na rotina administrativa

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas da Universidade. Os sistemas entre áreas, faculdades, e centros de gestão se comunicam entre si para que os objetivos institucionais da Universidade sejam concluídos com sucesso.

O art. 25 da LGPD, dispõe que os dados devem ser mantidos “em formato interoperável e estruturado para o uso compartilhado”, visando, entre outros objetivos, a prestação de serviços públicos, e a descentralização da atividade pública”. Significa dizer que o compartilhamento interno e externo de dados pessoais, para cumprimento das funções vinculadas à Universidade, é possível e possui fundamento na LGPD.

Mas ainda assim, é importante que o servidor sempre recorra a matriz do nosso ‘MAPA DE TRATAMENTO’(item VI desse GUIA). É preciso se certificar de que todo compartilhamento seja justificado.



REQUISITOS PARA O COMPARTILHAMENTO

O compartilhamento interno de dados pessoais pelos servidores deve observar, principalmente, as seguintes diretrizes:

- a definição de propósitos legítimos e específicos;
- a sua compatibilidade com as finalidades de tratamento vigentes no vínculo entre o titular e a Universidade;
- a limitação do compartilhamento de dados pessoais ao mínimo necessário para o atendimento da finalidade informada;
- o grau de sigilo que deve ser atribuído à informação compartilhada. Tanto para quem remete os dados, quanto quem os recebe, deverá aplicar regras de sigilo e confidencialidade (que já são praticadas), limitando o acesso para que o mesmo aconteça somente por outros servidores específicos e suas respectivas áreas.

COMPARTILHAMENTO POR E-MAIL

Sempre que dados pessoais forem solicitados, ainda que seja um pedido habitual, a partir de agora, solicite que seja enviado um e-mail, informando a finalidade para a qual aquela remessa de dados pessoais será utilizada, no qual conste:

- Qual o departamento de quem está solicitando;
- Qual o cargo de quem está solicitando;
- Qual a finalidade do tratamento daquele(s) dado(s) após o compartilhamento.

É importante que, de alguma forma, conste a

relação do titular de dados com a Universidade, pois isso representa o acordo – maior – que dará respaldo a todo o uso daquelas informações pessoais sob a responsabilidade da Universidade.

Pedidos entre áreas internas e externas que envolvam compartilhamento de dados pessoais, sob a responsabilidade da Universidade, precisam ser feitos por e-mail para que o servidor que fará a remessa das informações, tenha a evidência de que o compartilhamento segue o padrão e os requisitos envolvidos pelas normas de privacidade e proteção de dados, comentada neste guia e em função da LGPD.



USO SECUNDÁRIO DE DADOS PESSOAIS

Nas seções deste Guia, abordamos a importância da finalidade para a qual os dados coletados do titular serão utilizados pela Universidade, pois essa informação é fundamental para que haja o adequado registro das atividades que envolvem tratamento de dados pessoais.

Assim, a regra é que o titular tenha conhecimento prévio sobre como seus dados serão tratados e para quais finalidades. Quando falamos em uso

secundário de dados pessoais, estamos dizendo que, em algumas circunstâncias os dados coletados podem ser utilizados para finalidades secundárias, ou complementares que não tenham sido comunicadas diretamente ao titular.

É claro que isso, na verdade, é uma prerrogativa das atividades do poder público, que por sua vez possui alguma flexibilidade no uso das informações dos particulares, por atuar para o interesse e serviços públicos.

Um aspecto sempre deve estar presente no uso secundário. **Ele somente pode ser realizado**, para uma finalidade que seja compatível com a finalidade original. Isso porque é importante observar a compatibilidade entre o tratamento dos dados pessoais e aquelas finalidades que foram informadas ao titular.

DIVULGAÇÃO PÚBLICA DE DADOS PESSOAIS, POR SERVIDORES



Quando em função das atividades cotidianas o servidor precisar fazer um compartilhamento público de dados pessoais do banco de dados da Universidade, essa divulgação precisa estar assegurada por algumas condutas fundamentais. Lembrando sempre de que o servidor deverá recorrer ao MAPA DE TRATAMENTO DE DADOS (item VI deste GUIA), para verificar se essa divulgação preenche os requisitos legais. Abaixo, citamos as principais medidas:

- Priorizar a anonimização total ou parcial da identidade do titular. (quando isso não prejudicar a própria finalidade da divulgação);
- Colher o consentimento do titular de dados pessoais previamente, quando não for possível a anonimização;
- Divulgar apenas o que é necessário para atingir a finalidade de transparência da atividade pública;
- Evitar, totalmente, a divulgação de dados pessoais sensíveis.

LGPD NA UNICAMP

A Universidade dispõe de alguns canais com informações gerais sobre o assunto privacidade e proteção de dados pessoais:

dúvidas e sugestões - lgpd@unicamp.br
informações sobre a lei -
<https://epdp.unicamp.br>

REFERÊNCIA BIBLIOGRÁFICA

A Lei Geral de Proteção de Dados Pessoais - LGPD
- Lei nº 13.709, de 14 de agosto de 2018





UNICAMP



ESCRITÓRIO DE
PROTEÇÃO DE
DADOS PESSOAIS