

GUIA

LGPD na verificação de identidade

Cinco artigos do blog sobre o tratamento de dados pessoais na verificação: o legítimo interesse, o contrato entre controlador e operador, a anonimização, o incidente com dado biométrico e o ofício de autoridade.

NESTE GUIA

1. Legítimo interesse na LGPD: como montar o teste de balanceamento
2. Contrato controlador-operador: cláusulas que não podem faltar
3. Anonimização e pseudonimização: diferenças com consequência jurídica
4. Incidente com dado biométrico: o plano de resposta antes de precisar dele
5. Ofício pedindo dados de cliente: o que entregar e o que recusar

Gerado em 27 de setembro de 2026

Versão web: <https://unifokal.com/publicacoes#lgpd-na-verificacao-de-identidade>

Legítimo interesse na LGPD: como montar o teste de balanceamento

Publicado em 12 de setembro de 2026 · <https://unifokal.com/blog/legitimo-interesse-e-balanceamento>

O artigo 10 da LGPD parágrafo a parágrafo, as três fases do teste de balanceamento descritas pela ANPD e a regra do guia que vale só para dado de criança e adolescente.

Legítimo interesse é a base legal que aparece na política de privacidade quando nenhuma outra encaixa. É também a única hipótese do artigo 7º da Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que a lei manda registrar com destaque: o artigo 37 determina que controlador e operador mantenham registro das operações de tratamento que realizarem, "especialmente quando baseado no legítimo interesse".

Escrever a expressão no documento não cria a base. O que cria é uma análise concreta, feita antes do tratamento, comparando o interesse de quem trata com os direitos de quem é tratado. Essa análise tem nome no vocabulário da autoridade: teste de balanceamento.

Este texto percorre o artigo 10 da LGPD parágrafo a parágrafo e depois o modelo de teste descrito pela Autoridade Nacional de Proteção de Dados (ANPD) no guia orientativo sobre legítimo interesse, versão 1.0, de fevereiro de 2024. No fim, separa uma regra desse guia que vale só para dado de criança e adolescente e costuma ser repetida como se fosse geral.

O artigo 10, parágrafo por parágrafo

O caput não define a base legal, delimita o seu uso: o legítimo interesse do controlador "somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas". A lista seguinte é aberta e traz dois exemplos: o inciso I fala em apoio e promoção de atividades do controlador; o inciso II, em proteção do exercício regular dos direitos do titular ou prestação de serviços que o beneficiem, "respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais".

O parágrafo 1º restringe o volume: só os dados estritamente necessários para a finalidade pretendida podem ser tratados. O parágrafo 2º manda o controlador adotar medidas para garantir a transparência desse tratamento. O parágrafo 3º autoriza a autoridade nacional a

solicitar relatório de impacto à proteção de dados pessoais quando o fundamento for o interesse legítimo, observados os segredos comercial e industrial.

A exceção que decide tudo está no artigo 7º, inciso IX: a hipótese vale "exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". A base nasce condicionada, e a condição é uma comparação. Por isso ela não se sustenta sem a comparação escrita.

Onde o legítimo interesse não entra

O artigo 11 da LGPD lista as hipóteses para dado pessoal sensível e não repete o legítimo interesse. O guia da ANPD é explícito: é hipótese "não aplicável ao tratamento de dados pessoais sensíveis, haja vista a sua previsão apenas no art. 7º da LGPD, não tendo sido reproduzida no art. 11". Se o tratamento alcança dado sensível, a resposta está em outra hipótese do artigo 11, não numa versão reforçada do teste.

Para quem opera verificação de identidade, a hipótese vizinha é o artigo 11, inciso II, alínea "g": garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. O guia da ANPD registra que essa alínea segue sistemática similar à do legítimo interesse, porque também cede quando prevalecerem direitos e liberdades fundamentais do titular, e afirma que as orientações do documento, inclusive o teste, se aplicam a ela. O mesmo guia lembra que a finalidade da alínea "g" "deve ser interpretada restritivamente e descrita de forma objetiva e o mais detalhada possível". Quem desenha uma esteira de sinais antifraude precisa dessa descrição antes do primeiro sinal, e as bases para biometria estão em qual é a base legal para verificar identidade.

O que faz um interesse ser legítimo

O guia fixa três condições cumulativas: compatibilidade com o ordenamento jurídico, isto é, tratamento que não contraria, direta ou indiretamente, disposições legais nem princípios aplicáveis; lastro em situação concreta, real, clara e precisa, e não especulativa; e vinculação a finalidades legítimas, específicas e explícitas, descritas com detalhe suficiente para permitir a ponderação.

Sobre a legítima expectativa, que o artigo 10, inciso II, manda respeitar, o guia lista fatores de análise: relação prévia entre controlador e titular; fonte e forma da coleta, isto é, se os dados vieram do próprio titular, de fontes públicas ou de terceiros; contexto e período da coleta; e

compatibilidade da finalidade original com o tratamento posterior. É onde projetos de rastreamento costumam cair, como detalha o artigo sobre device fingerprinting e LGPD.

As três fases do teste

O modelo do Anexo II do guia divide o exame em três partes. Na fase 1, finalidade, verifica-se a natureza dos dados, identifica-se o interesse, se do controlador ou de terceiro, e avalia-se a sua legitimidade contra as três condições acima. Na fase 2, necessidade, pergunta-se se o tratamento é necessário para atingir o objetivo da fase anterior, se existem formas menos intrusivas ou com menores riscos, e se apenas os dados estritamente necessários estão em uso. Na fase 3, balanceamento e salvaguardas, avaliam-se riscos e impactos sobre direitos e liberdades fundamentais, as medidas de mitigação e de transparência e a existência de canal de fácil acesso para o titular se opor, se descadastrar ou pedir o término da operação.

Duas advertências do guia evitam expectativa errada. A primeira: não existe abordagem única, o teste pode ser breve quando o impacto aos direitos dos titulares é claramente baixo, e mais robusto no uso de novas tecnologias baseadas em quantidades massivas de dados pessoais; o modelo do Anexo II não é de uso obrigatório. A segunda: "o que a LGPD exige não é o impacto zero", e sim que impactos eventuais sejam minimizados e considerados na adoção de salvaguardas. Se o teste concluir pela prevalência dos direitos e das legítimas expectativas dos titulares, o tratamento não deve ser feito com essa base.

A regra que vale só para criança e adolescente

Aqui está a parte do guia mais citada fora do lugar. Na seção sobre dados pessoais de crianças e adolescentes, a ANPD afirma que o controlador deve elaborar teste de balanceamento e manter registro da justificativa capaz de demonstrar três coisas: o que foi considerado como melhor interesse da criança ou do adolescente; com base em quais critérios os direitos deles foram ponderados contra o interesse do controlador ou de terceiro; e que o tratamento não gera riscos ou impactos desproporcionais e excessivos.

Esses três itens são exigências desse recorte, não do legítimo interesse em geral. Decorrem do artigo 14 da LGPD, segundo o qual o tratamento de dados de crianças e adolescentes deve ser realizado em seu melhor interesse, e do Enunciado CD/ANPD nº 1, de 22 de maio de 2023, reproduzido no guia, que admite as hipóteses dos artigos 7º e 11 para esse público desde que observado e prevalecente o melhor interesse. Generalizar a lista é atribuir à autoridade uma exigência que ela escreveu em outro contexto.

Na mesma seção, o guia aponta o uso de dados de crianças e adolescentes como um dos critérios de alto risco fixados pela ANPD, com remissão ao artigo 4º da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, que aprova o regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte. Vale ler a norma citada: aquele artigo considera de alto risco, para os fins daquele regulamento, o tratamento que atende cumulativamente a pelo menos um critério geral e um critério específico, e o uso de dados de crianças, adolescentes e idosos aparece como critério específico, na alínea "d" do inciso II. Critério específico sozinho não fecha a classificação.

Perguntas frequentes

O teste de balanceamento é obrigatório por lei?

A LGPD não usa a expressão. O que a lei exige é o registro das operações de tratamento, com menção expressa ao legítimo interesse, no artigo 37, além dos deveres do artigo 10. O guia da ANPD diz que o tratamento com respaldo nessa base deve ser precedido do teste e o trata como instrumento para demonstrar conformidade, nos termos do artigo 6º, inciso X, e do artigo 37.

Quando o teste precisa virar relatório de impacto?

São documentos diferentes. O artigo 10, parágrafo 3º, permite à autoridade solicitar o relatório quando o fundamento for o legítimo interesse, e o artigo 38 prevê essa determinação em termos gerais. O guia observa que o relatório pode incorporar o teste, com análise mais ampla de riscos e mitigações. O roteiro está em [relatório de impacto para verificação biométrica](#).

Fontes citadas

- Lei 13.709/2018 (LGPD), artigos 6º, 7º, 10, 11, 14, 37 e 38, no portal do Planalto: planalto.gov.br
- ANPD, Guia orientativo "Hipóteses legais de tratamento de dados pessoais: legítimo interesse", versão 1.0, fevereiro de 2024, com os Anexos I e II: gov.br/anpd
- Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, artigo 4º, no Diário Oficial da União: in.gov.br

- Enunciado CD/ANPD nº 1, de 22 de maio de 2023, conforme reproduzido no guia de legítimo interesse da ANPD

Contrato controlador-operador: cláusulas que não podem faltar

Publicado em 1 de setembro de 2026 · <https://unifokal.com/blog/contrato-controlador-operador>

Quem contrata verificação de identidade é controlador; o fornecedor, operador. As cláusulas que a LGPD pressupõe nesse contrato, da instrução documentada ao destino dos dados no término.

Quando uma empresa contrata um fornecedor de verificação de identidade, ela não está só comprando tecnologia: está entregando dados pessoais dos próprios clientes, inclusive dados sensíveis como biometria, para outra organização tratar. A LGPD tem nomes para os dois lados dessa mesa e consequências para os dois, e o contrato entre eles é o documento que decide, com anos de antecedência, como as perguntas difíceis serão respondidas: quem avisa quem no incidente, quem atende o titular, o que acontece com os dados no fim.

Este artigo mapeia os papéis, a responsabilidade que a lei distribui e as cláusulas que um contrato controlador-operador de KYC precisa ter para proteger os dois lados, na ordem em que elas costumam faltar.

Quem é quem: os papéis do artigo 5º

A LGPD, Lei 13.709/2018, define no artigo 5º o controlador (inciso VI) como quem toma as decisões referentes ao tratamento, e o operador (inciso VII) como quem realiza o tratamento em nome do controlador. No arranjo típico de verificação de identidade, a empresa contratante é controladora: ela decide verificar seus usuários, com qual profundidade e para qual finalidade. O fornecedor é operador: verifica porque foi instruído, nos limites da instrução.

O artigo 39 dá a regra de ouro do arranjo: o operador realiza o tratamento segundo as instruções fornecidas pelo controlador, e cabe ao controlador verificar a observância dessas instruções. Duas obrigações numa frase: o operador não inventa finalidade, e o controlador não terceiriza a consciência. E o artigo 37 obriga ambos a manter registro das operações de tratamento que realizarem, o que o contrato deve refletir como obrigação recíproca, não como cortesia.

Por que o contrato importa: a responsabilidade é pegajosa

O artigo 42, parágrafo 1º, inciso I, estabelece que o operador responde solidariamente pelos danos quando descumprir as obrigações da legislação ou quando não seguir as instruções lícitas do controlador. A leitura de negócio: o operador que trata fora da instrução compra o passivo junto; o controlador que instrui mal, ou não instrui, não se esconde atrás do fornecedor. Nenhum contrato revoga a lei, mas é o contrato que prova qual era a instrução, e sem essa prova a discussão de responsabilidade vira arqueologia de e-mails.

As cláusulas, na ordem em que fazem falta

- Objeto e instruções documentadas. O que exatamente o operador faz com os dados, por escrito e versionado: módulos de verificação executados, categorias de dados tratadas, fontes consultadas. Instrução vaga ("prestar serviços de verificação") não orienta operação nem defende ninguém.
- Finalidade e vedação de uso próprio. Os dados servem à verificação instruída e a nada mais. A cláusula que veda ao operador usar os dados para fins próprios, inclusive treinar modelos ou enriquecer bases comerciais, é a que separa operador de sócio oculto do dado.
- Suboperadores. Quem o operador subcontrata (nuvem, comunicação, fontes de dados), com dever de transparência sobre a lista, obrigação de impor por escrito o mesmo regime de proteção e regras para mudanças. Sem essa cláusula, o controlador não sabe por quantas mãos o dado passa.
- Segurança e sigilo. As medidas do artigo 46 traduzidas em compromissos verificáveis, criptografia em repouso e em trânsito, controle de acesso, segregação por cliente, e o compromisso de confidencialidade do pessoal com acesso.
- Incidente de segurança. A lei põe o dever de comunicar à ANPD e ao titular na cabeça do controlador (artigo 48), mas quem detecta o incidente na infraestrutura é o operador. O contrato precisa criar o dever espelho, o operador avisa o controlador em prazo definido e curto, com informação suficiente para a avaliação de risco, porque o relógio regulatório de três dias úteis corre para o controlador, como detalha o artigo sobre incidente com dado biométrico.
- Atendimento aos titulares. Pedidos de acesso, correção e eliminação chegam ao controlador, mas parte das respostas mora nos sistemas do operador. Prazos e formato dessa colaboração entram no contrato, com a régua do que pode e do que não pode ser apagado descrita no artigo sobre direitos do titular em KYC.

- **Término:** devolução ou eliminação, com exceção nomeada. No fim da relação, os dados são devolvidos ou eliminados, ressalvada a guarda que a lei impõe, como os prazos regulatórios de retenção do setor financeiro. A exceção precisa estar escrita com fonte, senão o "guardamos por obrigação legal" vira licença genérica para reter tudo.
- **Verificação da observância.** Se o artigo 39 manda o controlador verificar as instruções, o contrato precisa dizer como: relatórios periódicos do operador, direito de solicitar evidências das medidas de segurança e prazo de resposta. Cláusula de verificação que não define mecanismo é promessa sem motor.
- **Encarregado e canais.** Os pontos de contato de proteção de dados dos dois lados, com a figura do encarregado descrita no artigo sobre o papel do DPO.

Antes de assinar: a diligência que o contrato não substitui

Cláusula boa não conserta fornecedor ruim. A avaliação técnica do operador, como ele armazena mídia, como segrega clientes, como trata subprocessadores, vem antes da assinatura e tem roteiro no artigo sobre como avaliar um fornecedor de KYC. E a decisão anterior a todas, se faz sentido operar verificação em casa assumindo o papel integral de controlador de biometria, tem a conta completa no artigo sobre construir ou comprar verificação.

O contrato controlador-operador é o documento menos glamouroso da contratação e o mais consultado da crise. Escrevê-lo bem custa uma tarde de trabalho conjunto entre jurídico e engenharia; escrevê-lo mal custa exatamente uma crise.

Fontes citadas

- Lei 13.709/2018 (LGPD), artigos 5º, 37, 39, 41, 42, 46 e 48, disponível no portal do Planalto: planalto.gov.br
- ANPD, Autoridade Nacional de Proteção de Dados, portal oficial, orientações a agentes de tratamento: gov.br/anpd

Anonimização e pseudonimização: diferenças com consequência jurídica

Publicado em 1 de setembro de 2026 · <https://unifokal.com/blog/anonimizacao-e-pseudonimizacao>

Anonimizado sai do escopo da LGPD, pseudonimizado não. As definições da lei, por que reidentificação é mais fácil do que parece e por que hash de CPF não anonimiza nada.

Existe uma frase que aparece em reunião de produto com a regularidade de um bug conhecido: "a gente anonimiza e pode usar". Na maioria das vezes, o que o sistema faz de verdade é trocar o nome por um código, guardar a tabela de correspondência e seguir tratando dado pessoal achando que não. A distância entre anonimizar e pseudonimizar parece semântica, mas é uma das fronteiras com mais consequência jurídica da LGPD: de um lado, dado fora do alcance da lei; do outro, dado pessoal com todas as obrigações de sempre.

Este artigo estabelece as definições pela letra da lei, mostra por que a reidentificação é mais fácil do que a intuição sugere, com os números dos estudos clássicos, e aterrissa no contexto de verificação de identidade: o que dá para anonimizar de verdade num sistema de KYC, e o que nunca vai dar.

O que a lei define, e onde

A LGPD, Lei 13.709/2018, define anonimização no artigo 5º, inciso XI: a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. O artigo 12 entrega a consequência: dados anonimizados não são considerados dados pessoais para os fins da lei, salvo quando o processo puder ser revertido com esforços razoáveis. É a única porta de saída do escopo da LGPD que não envolve eliminar o dado.

A pseudonimização é outra coisa, e a própria lei a define no artigo 13, parágrafo 4º: o tratamento por meio do qual um dado perde a possibilidade de associação direta ou indireta a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. A palavra decisiva é "senão": a ponte de volta existe, está guardada em algum lugar, e enquanto ela existir o dado segue sendo pessoal. Pseudonimizar é uma medida de segurança excelente e recomendável; o que ela não é, nunca, é uma saída do escopo da lei.

Reidentificação: os números que curam o otimismo

A intuição diz que remover nome e CPF de uma base a torna anônima. A pesquisa diz o contrário há décadas. Latanya Sweeney demonstrou no estudo Simple Demographics Often Identify People Uniquely (Universidade Carnegie Mellon, 2000) que 87% da população dos Estados Unidos era identificável de forma única pela combinação de apenas três atributos banais: código postal, data de nascimento e sexo. Nenhum dos três é "identificador" sozinho; juntos, apontam uma pessoa.

Arvind Narayanan e Vitaly Shmatikov levaram a lição às bases comportamentais no estudo Robust De-anonymization of Large Sparse Datasets (IEEE Symposium on Security and Privacy, 2008), reidentificando usuários da base "anônima" de avaliações de filmes do Prêmio Netflix por cruzamento com avaliações públicas em outro site: em base esparsa, o próprio padrão de comportamento é a impressão digital. A resposta acadêmica a esse problema, o conceito de k-anonimato proposto por Sweeney em 2002, exige que cada combinação de atributos indiretos apareça em pelo menos k registros, e mostra na prática o custo da anonimização honesta: ela destrói detalhe, e destruir detalhe é o preço.

O caso do hash de CPF, e por que ele engana

O exemplo brasileiro perfeito da confusão é o hash de CPF. Aplicar uma função de resumo criptográfico ao CPF parece anonimizar: o número vira uma sequência irreconhecível e a função não tem inversa. O problema é aritmético: o espaço de CPFs válidos é minúsculo para uma máquina, na casa de um bilhão de combinações, e qualquer um pode calcular o hash de todos eles e montar a tabela reversa completa em hardware comum. O resultado é, na melhor hipótese, uma pseudonimização sem a parte do "ambiente controlado e seguro", porque a informação adicional que reverte o processo é pública: o próprio algoritmo. Pela régua do artigo 12, reversão com esforços razoáveis descaracteriza a anonimização, e poucas coisas são tão razoáveis quanto uma tabela pré-computada.

A versão honesta desse desenho existe e é padrão em segurança: hash com chave secreta (HMAC), com a chave guardada separada e rotacionável. É útil, defensável e continua sendo pseudonimização: dado pessoal, dentro do escopo, com a ponte de volta trancada em vez de destruída.

No KYC: o que cada categoria pode ser

Aterrissando no fluxo de verificação de identidade, as três categorias convivem:

- O que permanece pessoal por natureza: o dossiê de verificação, a mídia, o vínculo entre CPF e decisão. É o coração do serviço e das obrigações regulatórias de guarda; não existe versão anônima de "quem é esta pessoa". Vale retenção com prazo e as réguas do artigo sobre retenção de dados de verificação.
- O que merece pseudonimização como higiene: identificadores em logs, referências internas entre sistemas, bases de análise interna. Reduz o dano de cada exposição acidental sem fingir que saiu da lei.
- O que pode ser anônimo de verdade: métricas agregadas com granularidade controlada, taxas de aprovação por período, distribuições de tempo de conclusão, desde que os recortes não afunilem em grupos pequenos o bastante para reidentificar, que é exatamente a lição do k-anonimato.

A fronteira também responde uma pergunta recorrente de atendimento a titular: eliminação a pedido, tratada no artigo sobre direitos do titular em KYC, não se satisfaz com pseudonimização, porque o dado segue pessoal. Chamar as coisas pelo nome certo, anônimo só o que não volta, é menos uma formalidade e mais a diferença entre uma arquitetura que se defende e uma que desmorona na primeira pergunta técnica da fiscalização.

Fontes citadas

- Lei 13.709/2018 (LGPD), artigos 5º, 12 e 13, disponível no portal do Planalto: planalto.gov.br
- Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3 (2000): dataprivacylab.org
- Arvind Narayanan e Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, IEEE Symposium on Security and Privacy (2008), preprint How To Break Anonymity of the Netflix Prize Dataset: arxiv.org/abs/cs/0610105
- Latanya Sweeney, k-anonymity: a model for protecting privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems (2002)

Incidente com dado biométrico: o plano de resposta antes de precisar dele

Publicado em 1 de setembro de 2026 · <https://unifokal.com/blog/incidente-com-dado-biometrico>

Rosto vazado não troca de senha. O que a LGPD e o regulamento de incidentes da ANPD exigem, por que biometria agrava o caso e o plano de resposta que se escreve em tempo de paz.

Quando um banco de senhas vaza, a resposta técnica existe e é rotineira: invalidar tudo, forçar redefinição, seguir em frente. Quando vaza um banco de selfies e documentos, essa resposta não existe. Ninguém redefine o próprio rosto. O dado biométrico comprometido fica comprometido para a vida do titular, e é essa assimetria que faz do incidente com biometria uma categoria própria, que merece plano próprio, escrito antes do dia em que for necessário.

Este artigo cobre as duas metades do problema para quem opera verificação de identidade: o que a norma brasileira exige quando o incidente acontece, e o que o desenho do sistema pode fazer, em tempo de paz, para que o incidente possível seja pequeno.

O que a lei exige: comunicação com relógio

A LGPD, Lei 13.709/2018, trata o tema em dois artigos que trabalham juntos. O artigo 46 exige medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou alteração. O artigo 48 cria o dever de comunicar: o controlador deve comunicar à ANPD, a Autoridade Nacional de Proteção de Dados, e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, com a comunicação descrevendo a natureza dos dados afetados, os titulares envolvidos, as medidas adotadas e os riscos relacionados.

O relógio e os critérios vieram com a Resolução CD/ANPD 15/2024, o regulamento de comunicação de incidente de segurança. Dois pontos do regulamento redesenham qualquer plano de resposta. Primeiro, o prazo: a comunicação à ANPD e aos titulares deve ocorrer em três dias úteis contados do conhecimento do incidente, prazo que só se cumpre com processo ensaiado. Segundo, o critério de relevância: entre os fatores que caracterizam o risco relevante está justamente o envolvimento de dados sensíveis, e dado biométrico usado para identificar uma pessoa é dado sensível por definição expressa do artigo 5º, inciso II, da LGPD.

Tradução operacional: vazamento de base biométrica dificilmente escapa do dever de comunicar. O regulamento ainda exige que todo incidente, comunicável ou não, seja registrado internamente com a avaliação que fundamentou a decisão.

Tempo de paz, parte um: saber onde o dado vive

Nenhum plano de resposta funciona sem o inventário: em quais sistemas existe mídia biométrica, por quais caminhos ela entra e sai, quem consegue acessá-la. Em arquiteturas de verificação bem desenhadas, a resposta é curta de propósito: a mídia vai direto do aparelho do usuário para o armazenamento de objetos por URL assinada de vida curta, cifrada em repouso, sem passar pelos servidores de aplicação nem se espalhar por logs, o desenho descrito no artigo sobre [upload seguro de mídia](#). Inventário curto é raio de explosão curto: no dia do incidente, a diferença entre "vazou o balde de mídia" e "não sabemos o que vazou" é a diferença entre uma comunicação precisa e uma crise sem fundo.

O segundo redutor de raio é a retenção: dado que já foi apagado não vaza. Cada mês a mais de mídia guardada além da necessidade é raio de explosão comprado de graça, e a régua de quanto guardar, por tipo de dado e obrigação legal, está no artigo sobre [retenção de dados de verificação](#).

Tempo de paz, parte dois: papéis e ensaio

O relatório de impacto à proteção de dados, o RIPD, exigível para tratamento de alto risco como biometria em escala, é o documento onde os cenários de incidente já deveriam estar pensados, com o roteiro descrito no artigo sobre [RIPD para verificação biométrica](#). E o encarregado de dados, figura do artigo 41 da LGPD detalhada no artigo sobre [o papel do DPO](#), é quem assina o canal com a ANPD e com os titulares: ele precisa estar no plano com nome, suplente e telefone, não como cargo abstrato. E quando a infraestrutura que guarda a mídia é de um fornecedor, o dever de o operador avisar o controlador em prazo curto precisa existir por escrito, cláusula tratada no artigo sobre o [contrato controlador-operador](#).

O plano em si cabe numa página: quem declara o incidente, quem congela e preserva evidência, quem avalia o risco pelo critério do regulamento, quem redige as comunicações, quem aciona o jurídico. O teste do plano é um exercício de mesa por semestre, com cenário concreto: credencial de leitura do armazenamento exposta, quantos registros, de quais

titulares, comunicamos ou não, com qual texto. Equipes que ensaiaram discutem conteúdo no dia do incidente; equipes que não ensaiaram discutem processo, e três dias úteis evaporam em discussão de processo.

As primeiras horas: conter, avaliar, comunicar

Na hora real, a sequência que o regulamento pressupõe é: conter o vetor (revogar credenciais, fechar o acesso, preservar logs), levantar a extensão (quais objetos, de quais titulares, em qual janela), avaliar a relevância do risco pelo critério normativo e decidir a comunicação com registro escrito da decisão. A tentação de esperar certeza completa antes de comunicar joga contra o prazo: o próprio regulamento admite comunicação complementar posterior, então a primeira comunicação vai com o que se sabe, dizendo o que ainda não se sabe.

Passada a crise, o ciclo fecha com a revisão: o que o incidente ensinou sobre inventário, acesso e retenção vira mudança concreta de arquitetura, com prazo e dono, e o registro interno documenta a lição junto com o caso.

Incidente com biometria não tem final feliz, tem final administrado. A diferença entre os dois desfechos raramente se decide no dia; decide-se nos meses anteriores, no inventário curto, na retenção enxuta e no ensaio que fez do plano um hábito em vez de um documento.

Fontes citadas

- Lei 13.709/2018 (LGPD), artigos 5º, 41, 46 e 48, disponível no portal do Planalto: planalto.gov.br
- Resolução CD/ANPD 15/2024, Regulamento de Comunicação de Incidente de Segurança, ANPD, publicada no Diário Oficial da União: in.gov.br
- ANPD, orientações sobre comunicação de incidente de segurança, portal oficial: gov.br/anpd

Ofício pedindo dados de cliente: o que entregar e o que recusar

Publicado em 3 de setembro de 2026 · <https://unifokal.com/blog/oficio-de-autoridade-e-dados-de-kyc>

Ordem judicial, requisição do Ministério Público, ofício de delegado e pedido de regulador têm regimes diferentes. Como autenticar, delimitar o escopo e registrar o atendimento.

Chega um e-mail com ofício timbrado pedindo "todos os dados" de um cliente verificado, prazo de quarenta e oito horas, menção a crime de desobediência. Quem opera verificação de identidade guarda imagem de documento, selfie, resultado de checagens e trilha de decisão, exatamente o acervo que investigação e fiscalização procuram.

As duas reações instintivas erram. Entregar tudo rápido é tratamento sem base legal e expõe dados de terceiros que nunca foram alvo. Negar em bloco invocando proteção de dados descumpra a lei quando a autoridade tem competência requisitória expressa.

Este artigo descreve prática de operação e não substitui parecer jurídico: todo ofício concreto passa pelo advogado da empresa.

Ordem judicial, requisição e ofício não são a mesma coisa

Tratar todo pedido como igual é a origem do erro nas duas direções.

- Ordem judicial é a porta larga. A Lei 12.965/2014, o Marco Civil da Internet, determina no artigo 10, parágrafo 1º, que o provedor só é obrigado a disponibilizar os registros mediante ordem judicial. Provocado pela parte interessada, o artigo 22 exige fundados indícios do ilícito, justificativa motivada da utilidade e o período dos registros.
- Autoridade policial e Ministério Público, em investigação criminal, têm alcance estreito. A Lei 9.613/1998, no artigo 17-B, dá acesso exclusivamente aos dados cadastrais do investigado que informem qualificação pessoal, filiação e endereço, sem autorização judicial, inclusive os mantidos por instituições financeiras e provedores de internet. A Lei 12.850/2013 repete a fórmula no artigo 15, e o Supremo Tribunal Federal, na Ação Direta de Inconstitucionalidade 4.906, de setembro de 2024, manteve o dispositivo e excluiu qualquer dado além desses três.

- Autoridade administrativa segue o artigo 10, parágrafo 3º, do Marco Civil, que ressalva os mesmos dados cadastrais aos órgãos com competência legal para requisitá-los. O Decreto 8.771/2016, no artigo 11, exige da autoridade o fundamento legal de competência expressa e a motivação, define dado cadastral como filiação, endereço e qualificação pessoal, isto é, nome, prenome, estado civil e profissão, e veda pedidos coletivos genéricos ou inespecíficos.
- Sigilo financeiro tem lei própria. A Lei Complementar 105/2001 manda as instituições financeiras conservarem sigilo em suas operações ativas e passivas e serviços prestados, com portas distintas: artigo 3º para o Poder Judiciário, artigo 4º para o Poder Legislativo Federal e as comissões parlamentares de inquérito, artigo 6º para autoridades fiscais com processo administrativo instaurado ou procedimento fiscal em curso.

Um fornecedor de tecnologia não é instituição financeira, mas seu cliente regulado é: o mesmo ofício muda de regime em cada ponta.

Autenticar o pedido antes de responder

Ofício falso é vetor conhecido de engenharia social: timbre é trivial de falsificar, número de processo inventado passa despercebido, e o prazo curto existe para impedir a conferência.

O mínimo são quatro passos. Conferir o número do processo ou do inquérito no sistema do tribunal, nunca no documento recebido. Ligar para o telefone institucional do site oficial, nunca o impresso no ofício. Conferir se o órgão tem previsão legal para requisitar aquilo. E, no caso administrativo, exigir o fundamento legal e a motivação que o artigo 11 do Decreto 8.771/2016 obriga a declarar.

Entregar exatamente o que foi pedido

O recorte é a pessoa requisitada, o período requisitado, os itens requisitados. Nada além.

O excesso não é cooperação, é infração. A Lei 13.709/2018, a LGPD, submete todo tratamento aos princípios de finalidade e necessidade do artigo 6º, e dado fora do alcance da requisição não tem finalidade que o sustente. Pior, o excesso carrega terceiros: um despejo bruto de sessão traz o operador que revisou o caso, endereços de IP de outras pessoas e imagem de fundo com gente que nunca foi investigada.

Pedido genérico do tipo "todos os dados que a empresa possua" merece resposta pedindo especificação: o decreto veda pedidos coletivos genéricos ou inespecíficos. E quando aqueles dados não são coletados, informe: o parágrafo 1º do mesmo artigo manda comunicar o fato à autoridade solicitante e dispensa o fornecimento.

Dado cadastral, registro e conteúdo têm portas distintas

A lei separa três camadas, e confundi-las é o que faz entregar de menos ou de mais.

Dado cadastral é a porta mais larga, limitada a qualificação pessoal, filiação e endereço, acessível a autoridade administrativa competente e à investigação criminal sem ordem judicial.

Registro de conexão e registro de acesso a aplicações, definidos no artigo 5º do Marco Civil, dependem da ordem judicial do artigo 10, parágrafo 1º, e têm prazos próprios, menores que o do acervo de verificação: um ano pelo artigo 13, dever do provedor de conexão, e seis meses pelo artigo 15, o dever de quem opera a aplicação. Os prazos estão detalhados na guarda de logs pelo Marco Civil.

A terceira camada é o conteúdo e o acervo de verificação: imagem do documento, selfie, dados extraídos, resultado biométrico. O artigo 10 do Marco Civil sujeita a guarda e a disponibilização de dados pessoais e de conteúdo de comunicações privadas à preservação da intimidade e da vida privada, e o parágrafo 2º condiciona o conteúdo de comunicações privadas a ordem judicial. É a camada mais protegida, e nenhuma porta administrativa a alcança: requisição de dado cadastral não autoriza entregar selfie, imagem de documento ou resultado biométrico. A hipótese da Lei Complementar 105/2001, artigo 1º, parágrafo 3º, inciso IV, pela qual não viola o sigilo a comunicação de ilícitos penais ou administrativos às autoridades competentes, é o caminho da comunicação espontânea feita pela instituição obrigada, não uma porta para atender ofício que pede o acervo.

Registrar o atendimento e decidir sobre o aviso ao titular

O artigo 37 da LGPD obriga controlador e operador a manter registro das operações de tratamento, e o artigo 6º, inciso X, positiva a prestação de contas. Responder a ofício é operação de tratamento, e a empresa precisará demonstrar que agiu certo.

O registro útil tem seis campos: quem pediu, o que foi pedido com o ofício anexado, o que foi entregue item a item, quando, quem autorizou e sob qual fundamento legal. Uma esteira bem desenhada registra quem consultou e quem exportou cada verificação, a evidência que

transforma suposição em prova.

Avisar o titular pode ser vedado ou postergado. Ele tem, pelo artigo 18 da LGPD, o direito de saber com quem seus dados foram compartilhados, assunto do artigo sobre direitos do titular em KYC. Mas o artigo 23 do Marco Civil permite ao juiz determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro, e a Lei 9.613/1998, no artigo 11, inciso II, manda a pessoa obrigada comunicar ao COAF, o Conselho de Controle de Atividades Financeiras, abstendo-se de dar ciência do ato a qualquer pessoa, inclusive àquela a que a informação se refira. Esse dever é do cliente regulado, não do fornecedor de tecnologia. A decisão é do jurídico, caso a caso, e o padrão seguro é não avisar antes dela.

A evidência acompanha o horizonte do acervo a que se refere. Para a instituição regulada, esse horizonte é o do artigo 67 da Circular BCB 3.978/2020: no mínimo dez anos de conservação das informações de conhecimento do cliente, contados do primeiro dia do ano seguinte ao fim do relacionamento.

Quem responde, e por que o fluxo vem antes do ofício

Improviso sob prazo curto produz a entrega errada, então o fluxo precisa estar escrito antes do primeiro ofício, com três papéis separados. O encarregado pelo tratamento de dados pessoais, do artigo 41 da LGPD, é o canal de contato e quem aciona o processo, com as atribuições descritas no artigo sobre o encarregado de dados. O jurídico decide o mérito. Operações executa a extração dentro do escopo aprovado, sem consulta livre ao banco.

O artigo 4º, inciso III, da LGPD afasta da lei o tratamento feito para fins exclusivos de segurança pública e de investigação e repressão de infrações penais, remetido a legislação específica pelo parágrafo 1º. Isso descreve o tratamento da autoridade e não dispensa a empresa privada de base legal para entregar: costuma ser o artigo 7º, inciso II, obrigação legal ou regulatória, ou o artigo 7º, inciso VI, exercício regular de direitos em processo judicial, administrativo ou arbitral. Nomear qual delas sustentou a entrega é parte da resposta.

Fontes citadas

- Lei 13.709/2018 (LGPD), arts. 4º, 6º, 7º, 18, 37 e 41: planalto.gov.br
- Lei 12.965/2014 (Marco Civil da Internet), arts. 5º, 10, 13, 15, 22 e 23: planalto.gov.br
- Decreto 8.771/2016, art. 11, sobre requisição de dados cadastrais: planalto.gov.br
- Lei Complementar 105/2001, arts. 1º, 3º, 4º e 6º, sigilo bancário: planalto.gov.br

- Lei 9.613/1998, arts. 11 e 17-B: planalto.gov.br
- Lei 12.850/2013, art. 15, sobre organização criminosa: planalto.gov.br
- Circular BCB 3.978/2020, art. 67: [site do Banco Central](http://site.do.Banco.Central)
- Supremo Tribunal Federal, Ação Direta de Inconstitucionalidade 4.906, julgada em 11 de setembro de 2024: portal.stf.jus.br

Sobre este guia

Este guia reúne, sem alteração de texto, artigos do blog da UNIFOKAL, plataforma brasileira de verificação de identidade. O endereço original de cada artigo está logo abaixo do título dele, e as fontes citadas continuam no fim de cada um.

A versão web deste guia, com os artigos atualizados, fica em <https://unifokal.com/publicacoes#lgpd-na-verificacao-de-identidade>.