

LGPD: O
QUE VOCÊ
PRECISA
SABER?



Bem-vindos ao Implementando a LGPD!

Por Jerusa Bohrer



Olá, pessoal!

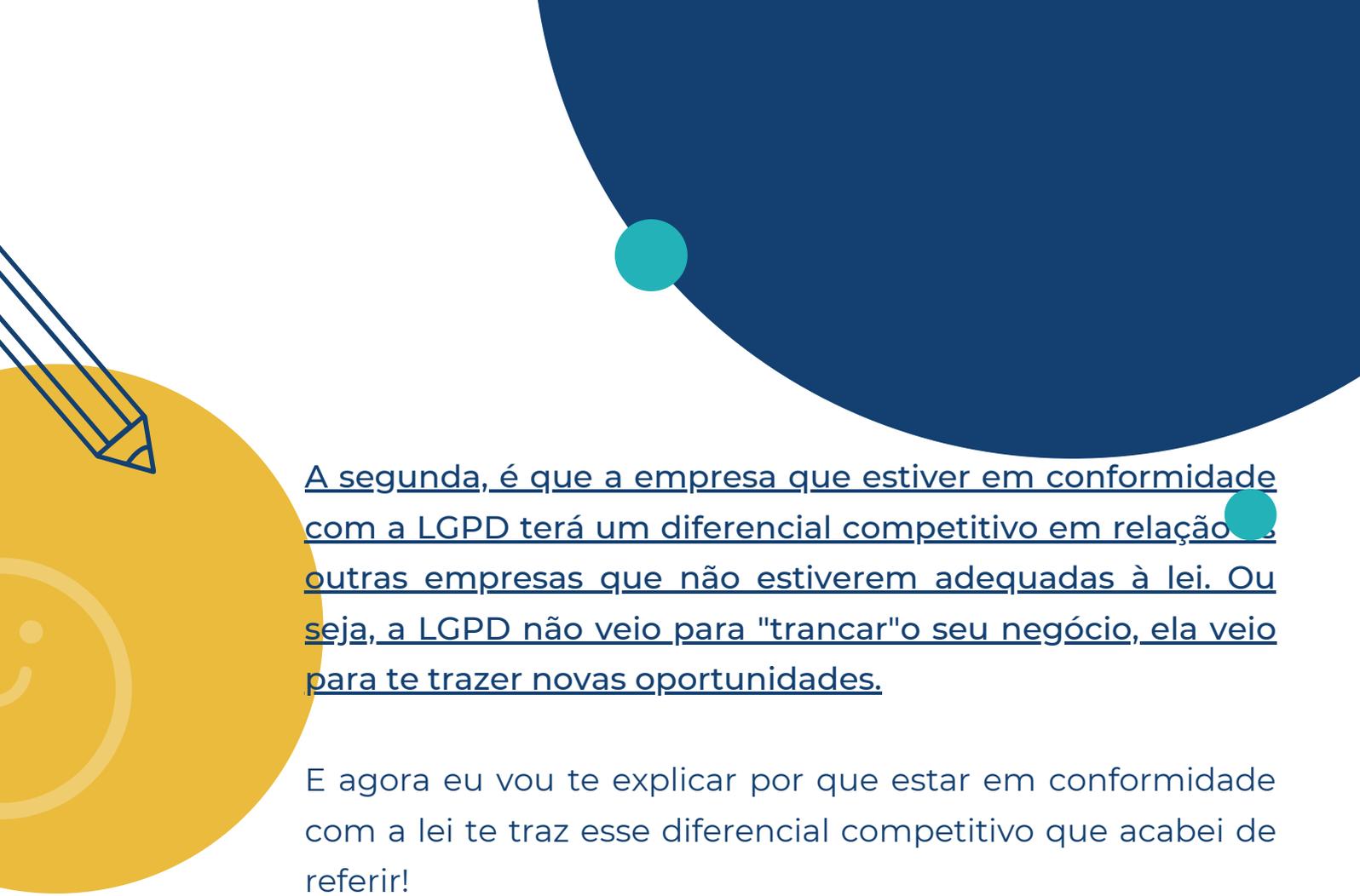
Tudo bem?

Se você está acessando este material é porque você estava na minha live, se interessa e entende a importância da LGPD. Ou seja, você e/ou sua empresa já estão um passo à frente das demais!

E se você chegou até aqui, eu assumo o compromisso de te ajudar nessa jornada de entendimento sobre a Lei Geral de Proteção de Dados, de forma simples, sem os termos técnicos e rebuscados geralmente utilizados pelos profissionais do Direito.

Mas antes de iniciar essa leitura que preparei especialmente para que você compreenda alguns dos principais pontos da Lei Geral de Proteção de Dados e ao final consiga entender quais os passos para a adequação da sua empresa, eu queria te falar algumas coisas bem importantes sobre a LGPD, que talvez você não saiba ou que possa ter compreendido de outra forma ao ouvir falar superficialmente sobre esta lei por aí.

A primeira coisa que eu quero te falar sobre a LGPD, é que ela não veio para acabar com as empresas, para inviabilizar alguns modelos de negócios ou para proibir que os dados pessoais sejam utilizados pelas empresas.



A segunda, é que a empresa que estiver em conformidade com a LGPD terá um diferencial competitivo em relação às outras empresas que não estiverem adequadas à lei. Ou seja, a LGPD não veio para "trancar" o seu negócio, ela veio para te trazer novas oportunidades.

E agora eu vou te explicar por que estar em conformidade com a lei te traz esse diferencial competitivo que acabei de referir!



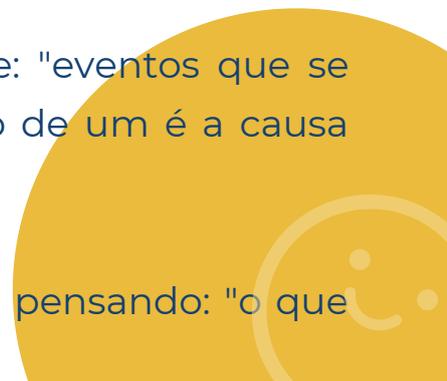
A "equação" é tão simples que você vai pensar: "como eu não me dei conta disso tudo antes?"

Você vai desejar ter começado a sua busca antes!

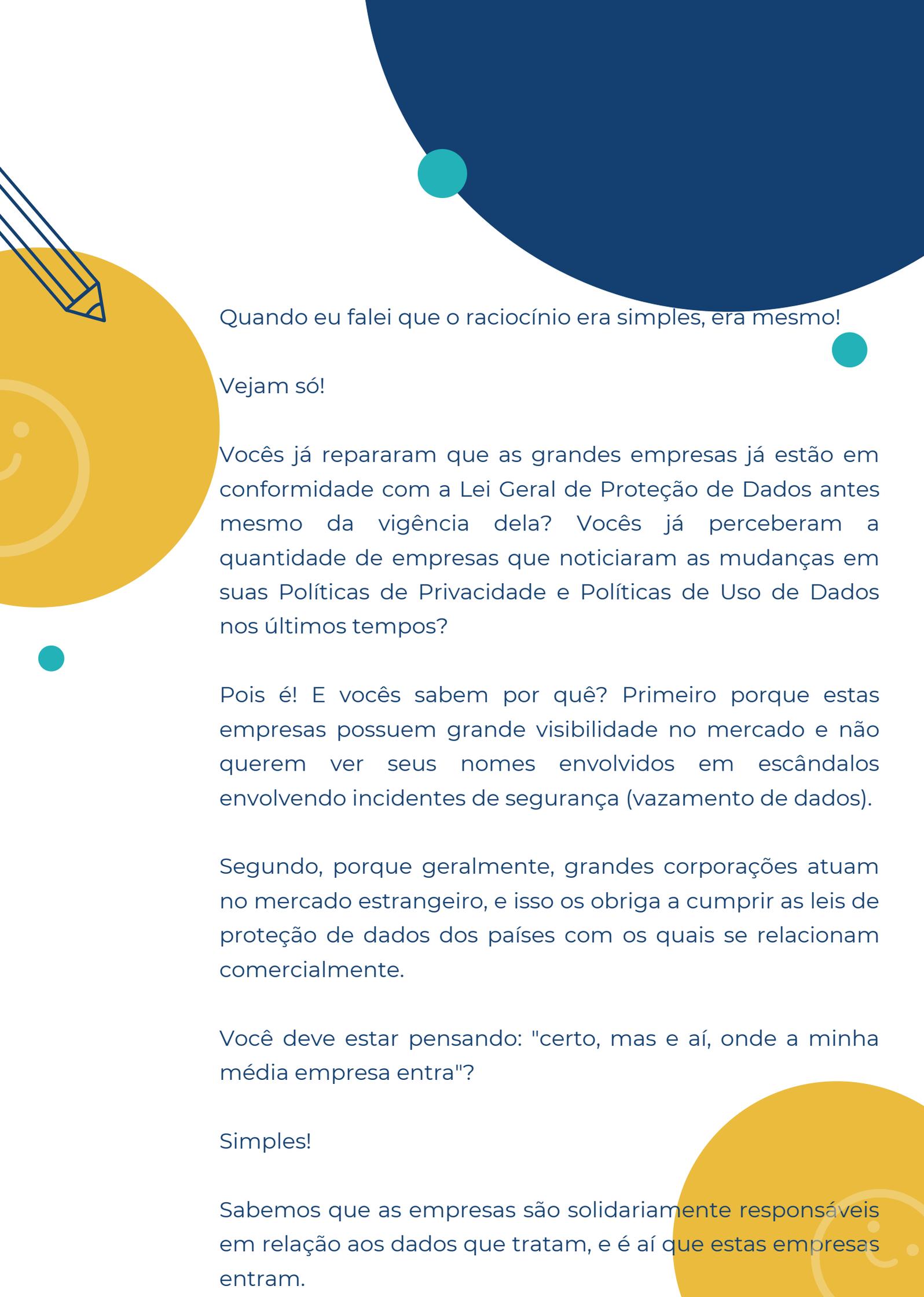
Você já ouviu falar em "efeito dominó ou em cadeia?"

De acordo com a definição do Wikipédia, o "efeito dominó, efeito em cascata ou efeito em cadeia sugere a ideia de um efeito ser a causa de outro efeito, gerando uma série de acontecimentos semelhantes de média, longa ou infinita duração".

Já a definição do dicionário é a seguinte: "eventos que se sucedem em cadeia, em que o resultado de um é a causa do outro; efeito cascata".



Conseguiram "matar a charada" ou estão pensando: "o que será que ela quer nos falar com isso?"



Quando eu falei que o raciocínio era simples, era mesmo!

Vejam só!

Vocês já repararam que as grandes empresas já estão em conformidade com a Lei Geral de Proteção de Dados antes mesmo da vigência dela? Vocês já perceberam a quantidade de empresas que noticiaram as mudanças em suas Políticas de Privacidade e Políticas de Uso de Dados nos últimos tempos?

Pois é! E vocês sabem por quê? Primeiro porque estas empresas possuem grande visibilidade no mercado e não querem ver seus nomes envolvidos em escândalos envolvendo incidentes de segurança (vazamento de dados).

Segundo, porque geralmente, grandes corporações atuam no mercado estrangeiro, e isso os obriga a cumprir as leis de proteção de dados dos países com os quais se relacionam comercialmente.

Você deve estar pensando: "certo, mas e aí, onde a minha média empresa entra"?

Simples!

Sabemos que as empresas são solidariamente responsáveis em relação aos dados que tratam, e é aí que estas empresas entram.



Vejam só o que diz o Art. 42:

"O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

O Art. 43 prevê:

"Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.



Percebem que se uma grande empresa possui relações comerciais com uma média empresa e está adequada à LGPD ela vai exigir desta média empresa a conformidade?

Porque a lógica aqui é simples: se esta grande empresa está em conformidade, ela não vai querer correr o risco de manter relações comerciais com uma empresa que não esteja aderente à lei, com uma empresa que não se preocupa com privacidade e proteção de dados dos seus clientes, porque em caso de incidente, ambas podem responder pelos danos.

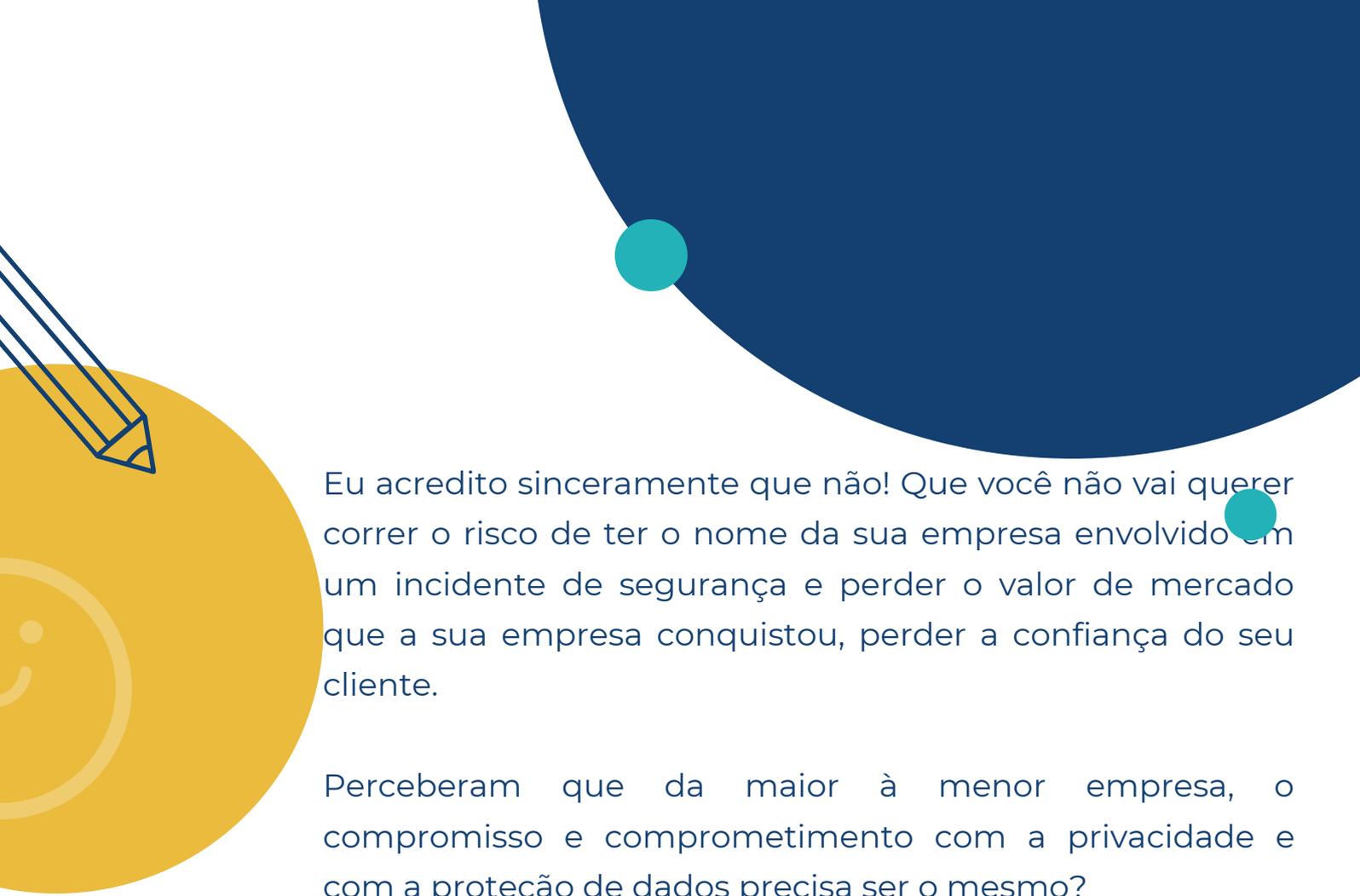
E, como consequência, é bem possível que a média empresa não faça mais negócios com esta grande empresa.

Outro ponto que merece atenção é que como a responsabilidade entre controlador e operador é solidária, se a pequena empresa se envolver em um incidente de segurança, a sua média empresa responderá com ela e, se eventualmente alguma sanção for aplicada, se estenderá à sua média empresa. Mesmo que a lei assegure o direito de regresso, você já pensou que talvez a pequena empresa não disponha de recursos para devolver o valor que a sua empresa pagou indevidamente?

E o "efeito dominó" ou em "cadeia" não para por aí.

Você é uma média empresa e agora, de olho no movimento do mercado e buscando o seu crescimento, já se adequou à LGPD, você vai querer se relacionar com uma pequena empresa que ainda não está em conformidade com a lei?





Eu acredito sinceramente que não! Que você não vai querer correr o risco de ter o nome da sua empresa envolvido em um incidente de segurança e perder o valor de mercado que a sua empresa conquistou, perder a confiança do seu cliente.

Perceberam que da maior à menor empresa, o compromisso e comprometimento com a privacidade e com a proteção de dados precisa ser o mesmo?



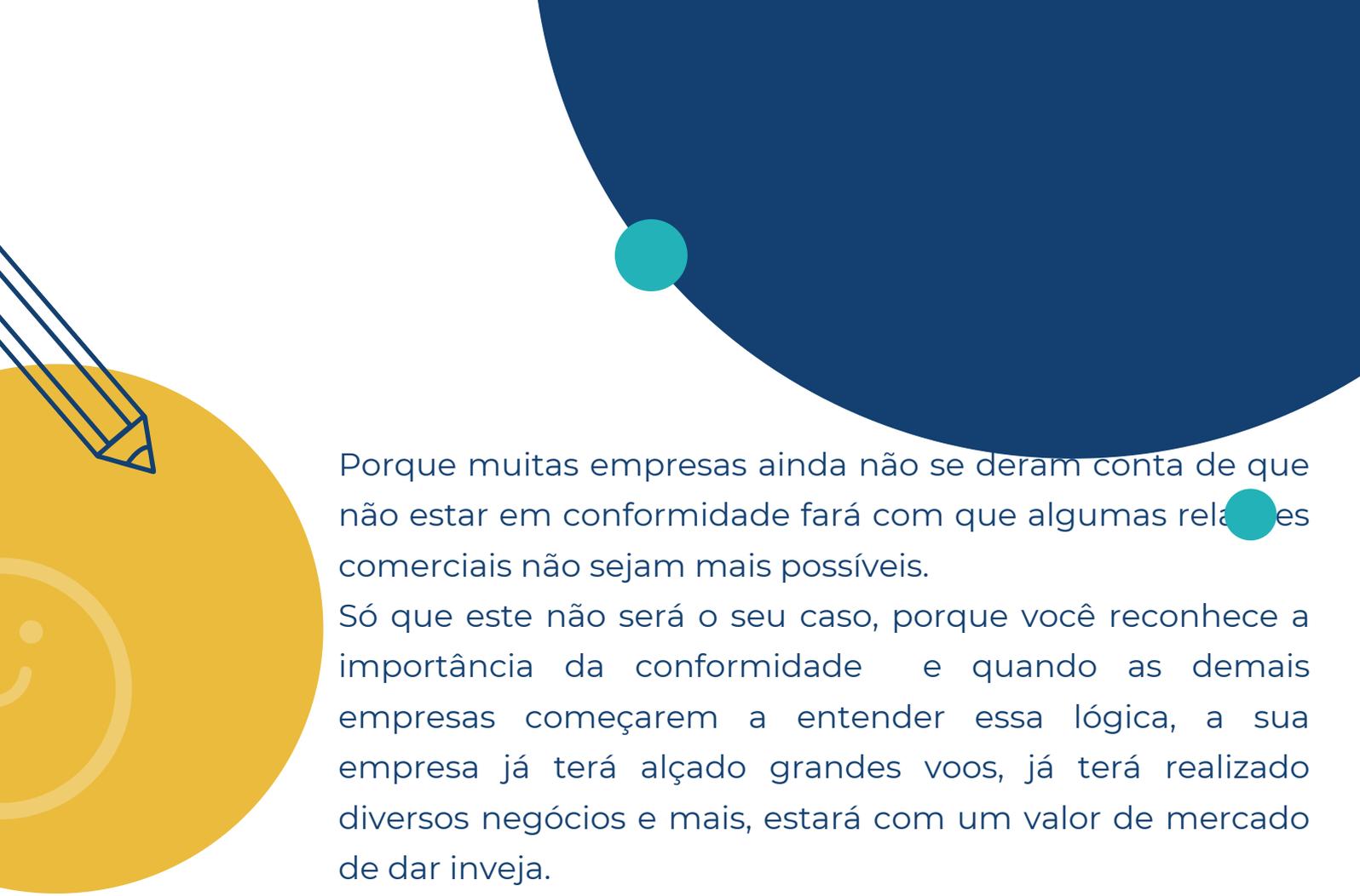
Esse é o sentido desta analogia, que a causa de um é o efeito do outro, e que essa relação causa e efeito pode trazer consequências para os envolvidos.

E nesse contexto, sabemos que muitas vezes as pequenas e médias empresas dependem de relações comerciais com grandes corporações para a continuidade de suas atividades, e elas precisarão se adequar. Ou seja, é um efeito que começa de cima e que vai se estendendo às médias e pequenas empresas que não terão outra opção que não seja a conformidade.

Além do "efeito dominó" você conseguiu perceber por que a conformidade da sua empresa com a LGPD é um diferencial competitivo?

Esta ficou fácil, né?





Porque muitas empresas ainda não se deram conta de que não estar em conformidade fará com que algumas relações comerciais não sejam mais possíveis.

Só que este não será o seu caso, porque você reconhece a importância da conformidade e quando as demais empresas começarem a entender essa lógica, a sua empresa já terá alçado grandes voos, já terá realizado diversos negócios e mais, estará com um valor de mercado de dar inveja.

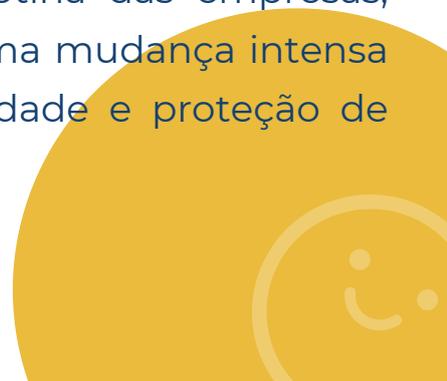


Lembra lá no início que eu falei que você já estava um passo à frente?!

Agora que você já está um passo à frente, eu te convido para dar o segundo passo, e para isso, quero compartilhar contigo os principais pontos da Lei Geral de Proteção de Dados.

Meu objetivo aqui não é esgotar a legislação, o que eu quero de verdade é que você compreenda e tenha domínio dos pontos mais relevantes desta legislação que veio para tutelar os direitos e garantias fundamentais dos titulares de dados e trazer alguns impactos na rotina das empresas, principalmente pela necessidade de uma mudança intensa na cultura delas em relação à privacidade e proteção de dados.

Vamos lá?





O que é LGPD e qual o seu objetivo?

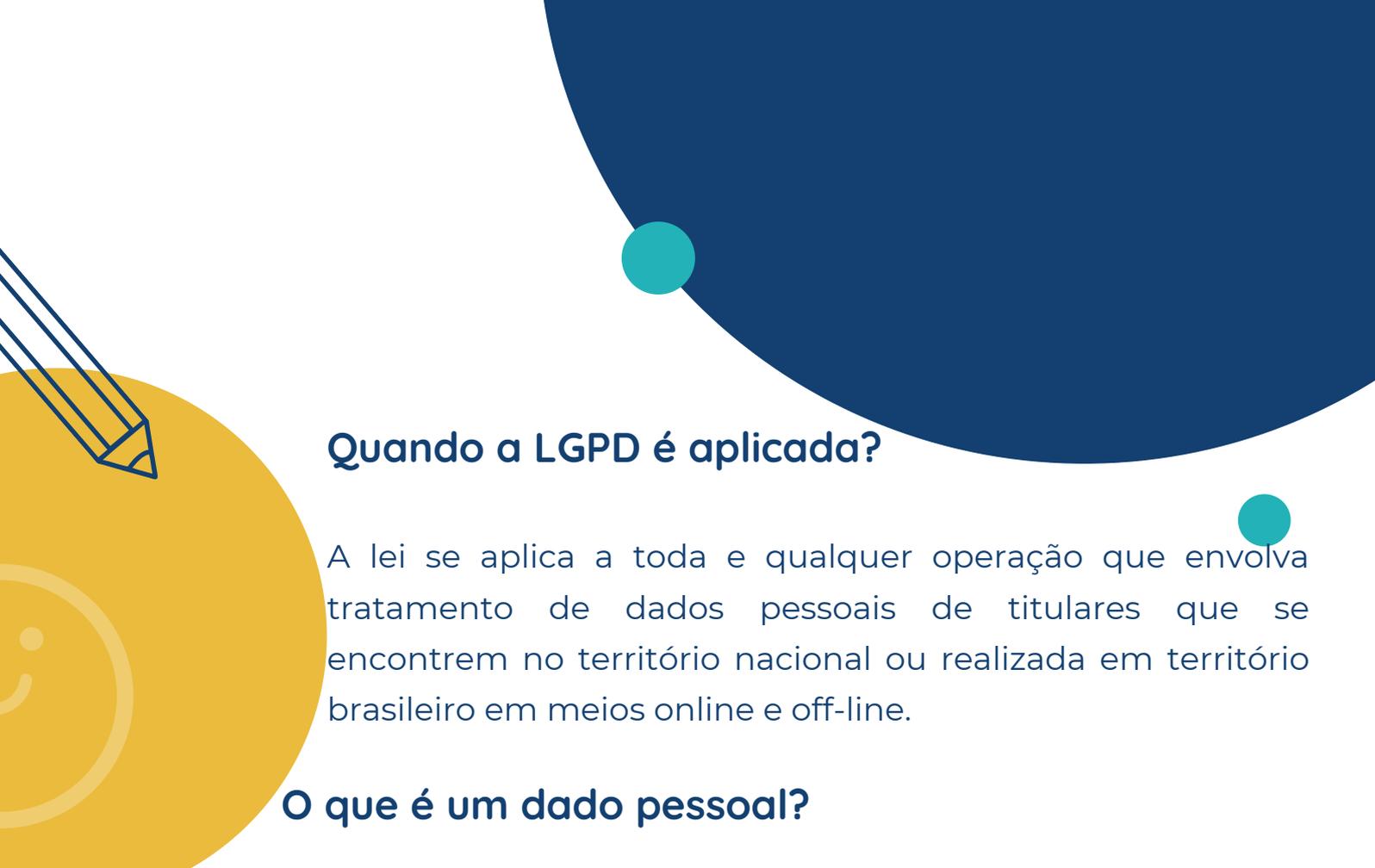
A Lei Geral de Proteção de Dados (Lei 13.709/18 ou LGPD), é uma Lei que veio para regulamentar os procedimentos a serem adotados em relação à privacidade e proteção dos dados pessoais.

Essa lei foi criada com o objetivo de fazer com que o usuário (titular dos dados) tenha um maior controle sobre a forma como seus dados são tratados, afinal, vivemos a era da sociedade da informação, onde os dados são a moeda da economia digital.

Por isso, a lei trouxe em suas disposições uma série de princípios, bases legais e demais regras que deverão ser observadas pelas empresas públicas e privadas ao realizarem atividades que envolvam tratamento de dados pessoais, para que de um lado garantam os direitos dos titulares, e de outro, continuem fomentando o desenvolvimento econômico. É o famoso ganha-ganha!

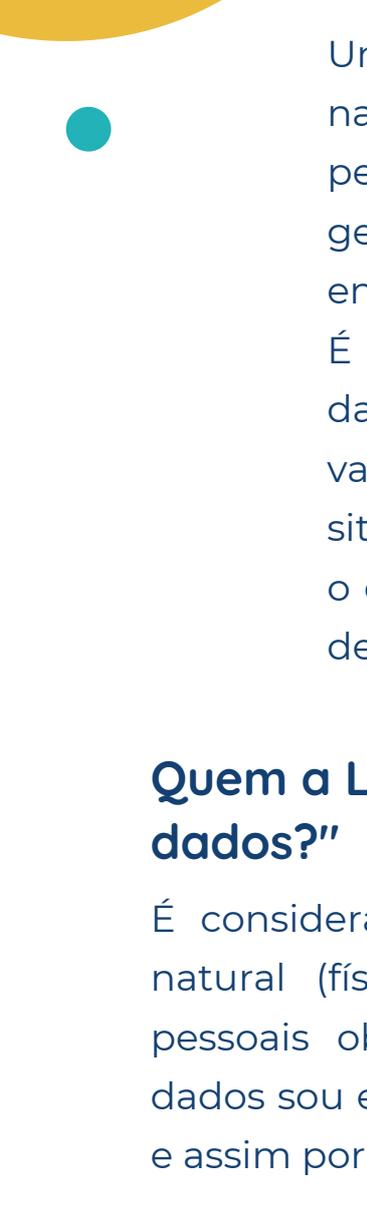
Quem está no escopo de aplicabilidade da LGPD?

Deverão estar em conformidade com a Lei Geral de Proteção de Dados toda pessoa natural ou jurídica de direito público ou privado que em suas atividades realize tratamento de dados pessoais, tanto em meios físicos como nos meios digitais.



Quando a LGPD é aplicada?

A lei se aplica a toda e qualquer operação que envolva tratamento de dados pessoais de titulares que se encontrem no território nacional ou realizada em território brasileiro em meios online e off-line.



O que é um dado pessoal?

Um dado pessoal é toda a informação relacionada à pessoa natural identificada ou identificável. São exemplos de dado pessoal: nome, endereço, telefone, e-mail, dados de geolocalização número do CPF, data de nascimento, endereço residencial, e-mail, etc..

É muito importante que você tenha a consciência de que dado pessoal é isso, mas não é somente isso, e essa análise vai depender do caso a caso, do contexto em que determina situação se insere. A LGPD não trouxe um rol taxativo sobre o que considera um dado pessoal, e por isso a necessidade desta análise em cada caso.

Quem a Lei considera "titular de dados?"

É considerado titular de dados toda a pessoa natural (física) a quem se referem os dados pessoais objeto do tratamento. Um titular de dados sou eu, é você, seu colaborador, seu cliente e assim por diante.





O que é um dado anônimo ou anonimizado?

Dado anônimo ou anonimizado é qualquer dado pessoal que quando submetido a meios técnicos razoáveis, não seja mais possível identificar ou possibilitar a identificação de uma pessoa natural, de forma direta ou indireta e de maneira irreversível.

O que é um dado pessoal sensível?

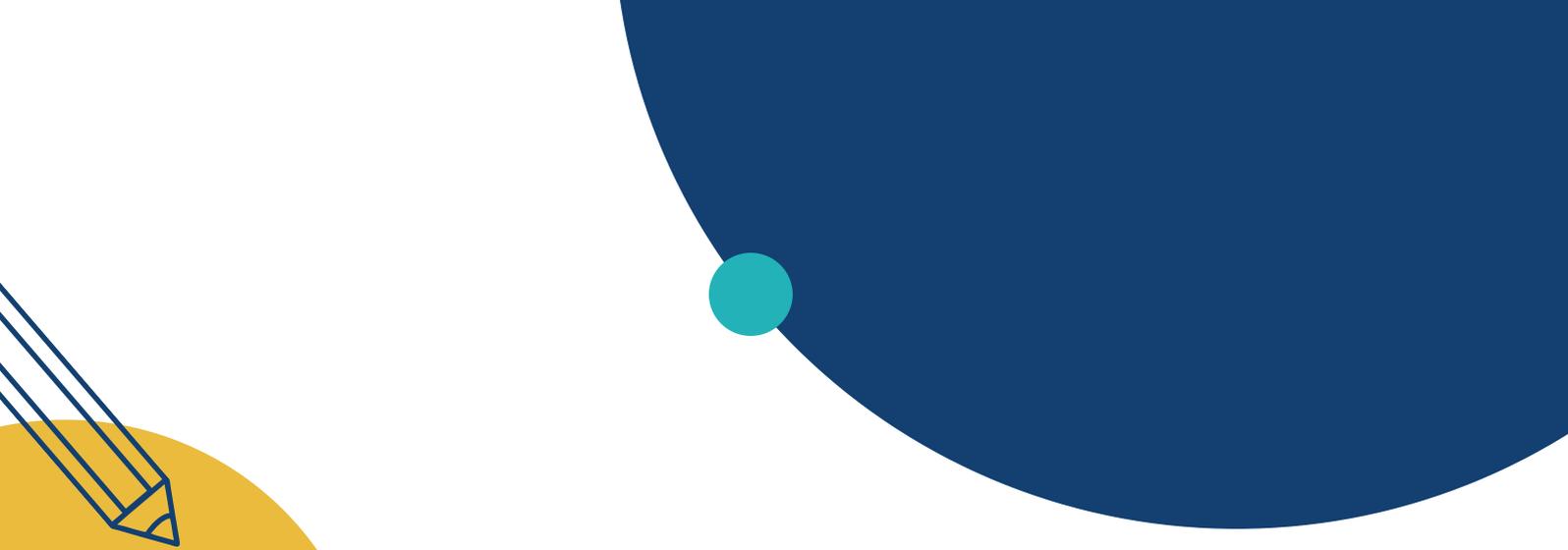
Um dado pessoal sensível é uma informação relacionada à pessoa natural identificada ou identificável, sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político. Também é considerado um dado sensível a informação relacionada à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado à pessoa natural.

Quem fiscalizará?

A fiscalização ocorrerá pela Autoridade Nacional de Proteção de Dados (ANPD). Além da fiscalização no que diz respeito ao cumprimento da lei, este órgão será responsável por zelar pela proteção de dados pessoais, elaborar diretrizes, bem como aplicar as sanções em casos de comprovadas irregularidades. Lembramos, entretanto, que a ANPD não possui competência exclusiva, tendo em vista que o Ministério Público também é competente com as questões relacionadas aos direitos dos cidadãos no que diz respeito aos direitos constitucionalmente previstos.

Quem é a Autoridade Nacional de Proteção de Dados (ANPD)?

A Autoridade Nacional de Proteção de Dados ou ANPD é um órgão da administração pública federal com autonomia técnica e decisória, integrante da Presidência da República, responsável por fiscalizar e garantir o cumprimento da lei, bem como aplicar sanções administrativas em caso de descumprimento. A ANPD caberá a interpretação da Lei e o estabelecimento de padrões e técnicas aplicáveis às questões de segurança da informação, interoperabilidade e processos de anonimização, dentre as demais atribuições dispostas no art. 55-J. A ANPD foi criada dia 27/08/2020, por meio do Decreto 10.474/2020, que aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados.



O que é considerado tratamento de dados?

Toda a operação realizada com dados pessoais, como por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



O que a LGPD considera compartilhamento de dados pessoais?

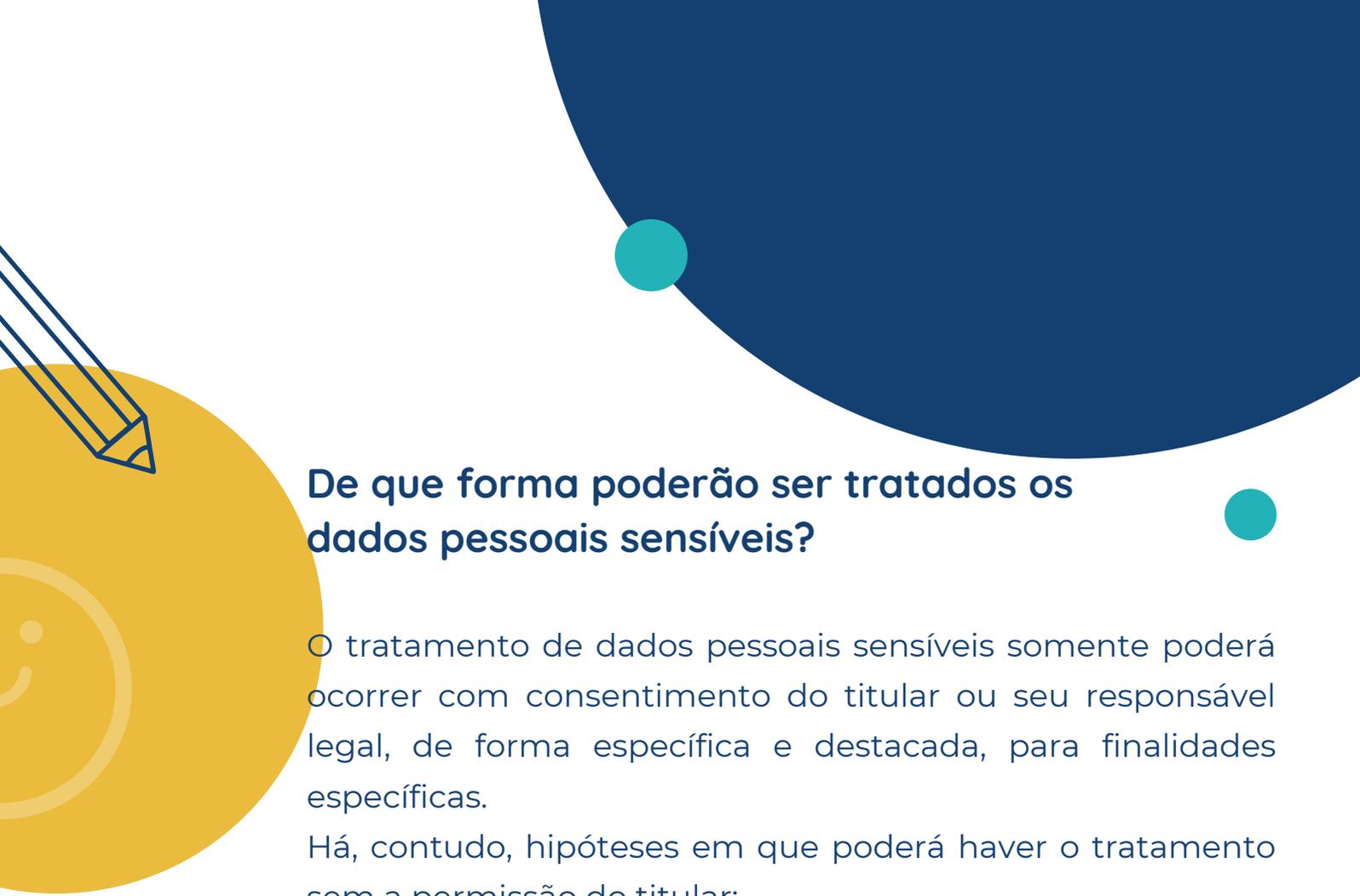
O compartilhamento de dados pessoais é toda a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados entre órgãos e entidades públicas no cumprimento de suas competências legais, ou entre tais órgãos e entes privados.



Quando os dados pessoais sensíveis poderão ser compartilhados?

A lei determina que os dados pessoais sensíveis deverão ser compartilhados com o consentimento expresso do titular. Entretanto, ele prevê exceções ao autorizar o compartilhamento destes dados sem o consentimento do titular de dados, sempre que necessário à adequada prestação de serviços de saúde suplementar, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia.

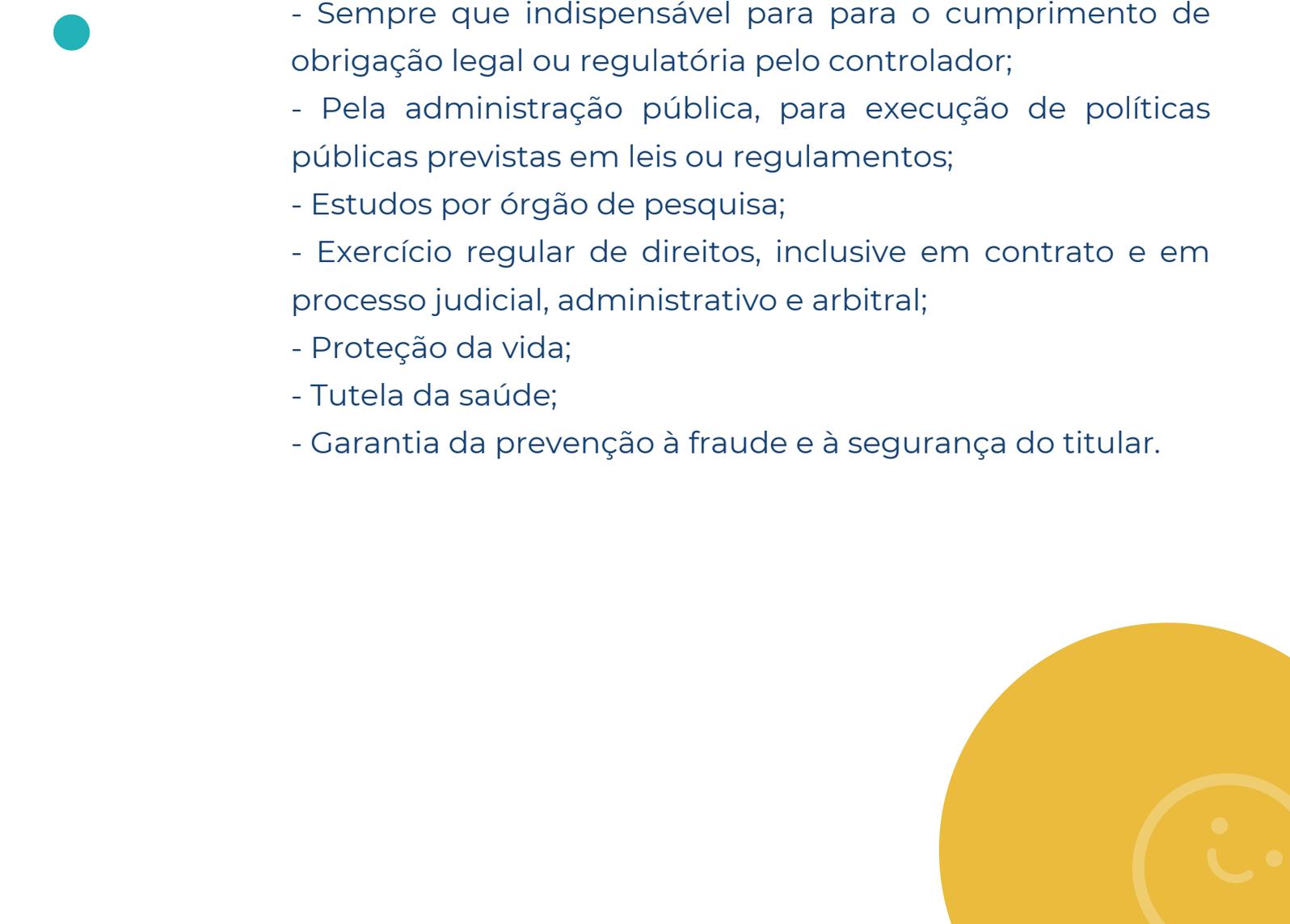


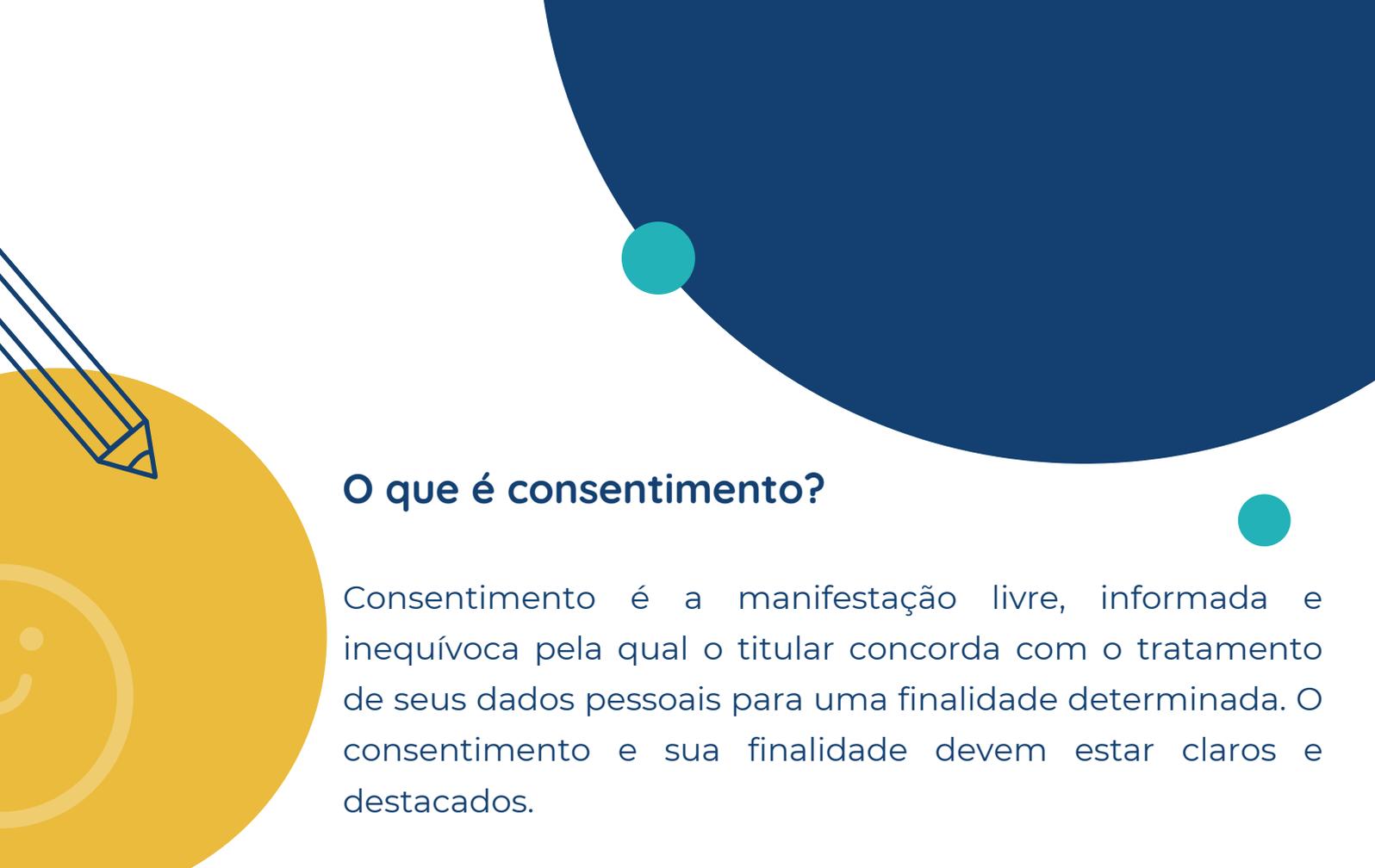


De que forma poderão ser tratados os dados pessoais sensíveis?

O tratamento de dados pessoais sensíveis somente poderá ocorrer com consentimento do titular ou seu responsável legal, de forma específica e destacada, para finalidades específicas.

Há, contudo, hipóteses em que poderá haver o tratamento sem a permissão do titular:

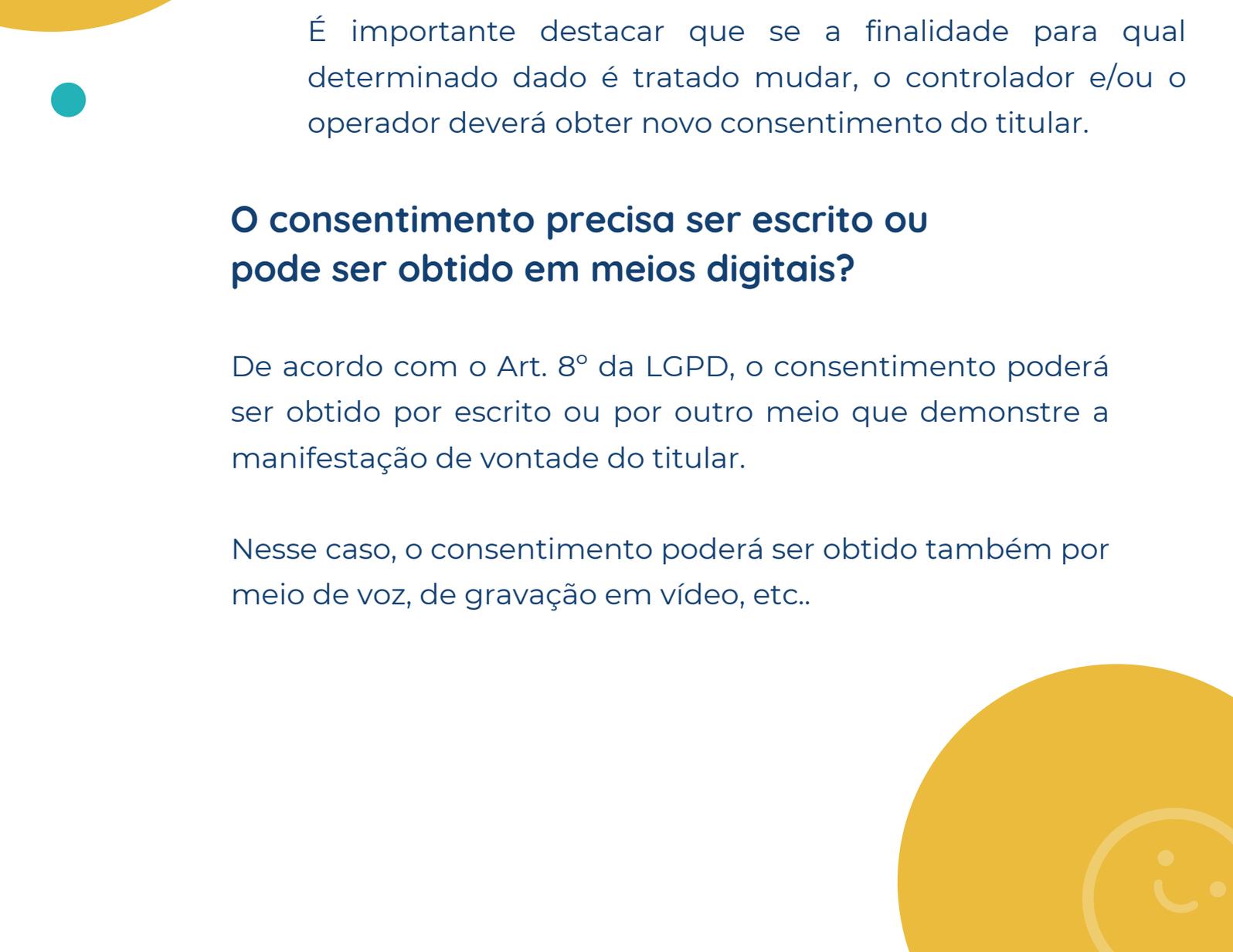
- Sempre que indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador;
 - Pela administração pública, para execução de políticas públicas previstas em leis ou regulamentos;
 - Estudos por órgão de pesquisa;
 - Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
 - Proteção da vida;
 - Tutela da saúde;
 - Garantia da prevenção à fraude e à segurança do titular.
- 



O que é consentimento?

Consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento e sua finalidade devem estar claros e destacados.

É importante destacar que se a finalidade para qual determinado dado é tratado mudar, o controlador e/ou o operador deverá obter novo consentimento do titular.



O consentimento precisa ser escrito ou pode ser obtido em meios digitais?

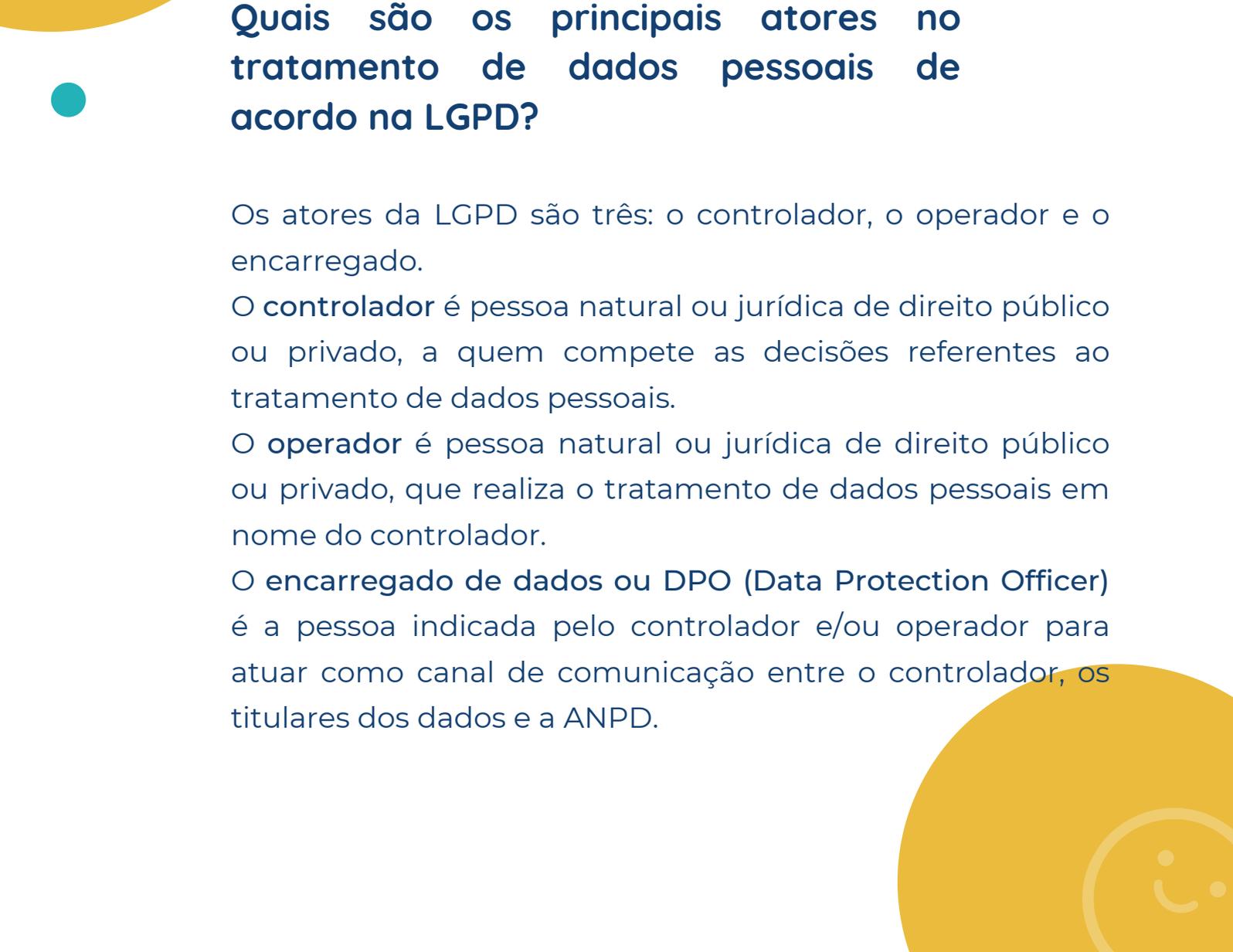
De acordo com o Art. 8º da LGPD, o consentimento poderá ser obtido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Nesse caso, o consentimento poderá ser obtido também por meio de voz, de gravação em vídeo, etc..



O titular dos dados pode revogar seu consentimento?

Sim. Dentre os direitos do titular que a LGPD estabelece está a revogação do consentimento, que poderá ocorrer a qualquer momento, quando solicitado pelo titular.



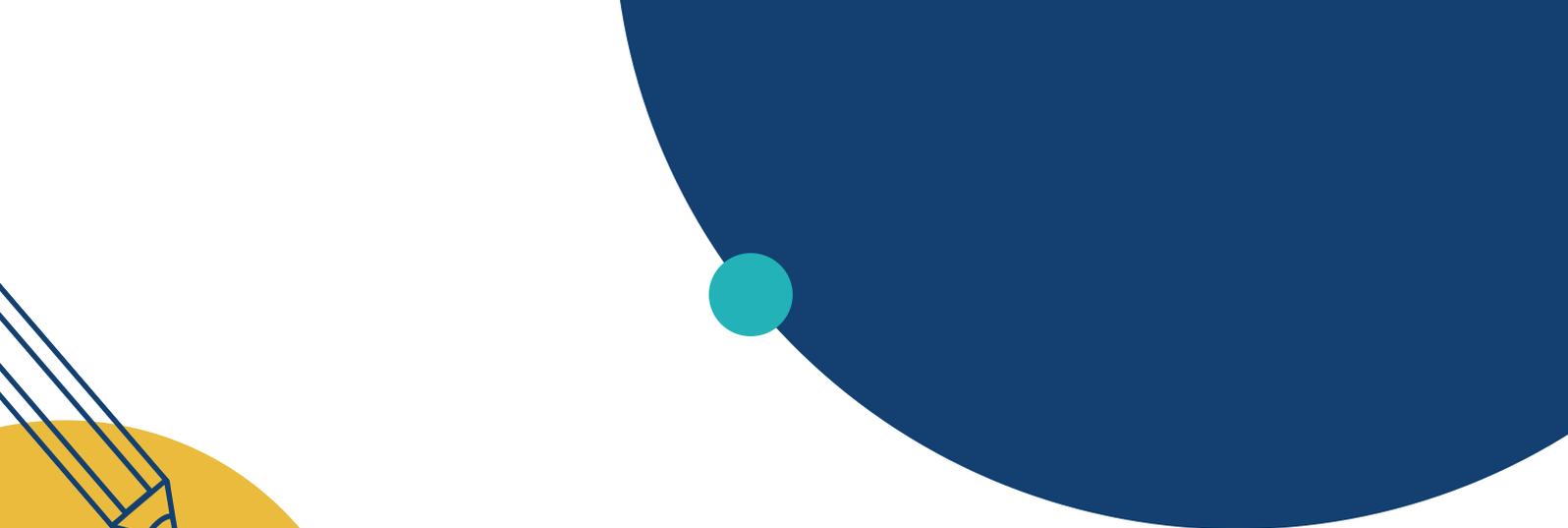
Quais são os principais atores no tratamento de dados pessoais de acordo na LGPD?

Os atores da LGPD são três: o controlador, o operador e o encarregado.

O **controlador** é pessoa natural ou jurídica de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

O **operador** é pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O **encarregado de dados ou DPO (Data Protection Officer)** é a pessoa indicada pelo controlador e/ou operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.



Esta Lei se aplica somente ao tratamento realizado na Internet?

Não. A LGPD é aplicável a qualquer operação de tratamento de dados pessoais realizada dentro do território brasileiro ou que tenha como objetivo oferecer bens ou serviços a pessoas localizadas no Brasil, independentemente destes dados pessoais terem sido coletados em meios físicos ou digitais.



Quem é o Encarregado de Dados ou DPO (Data Protection Officer)

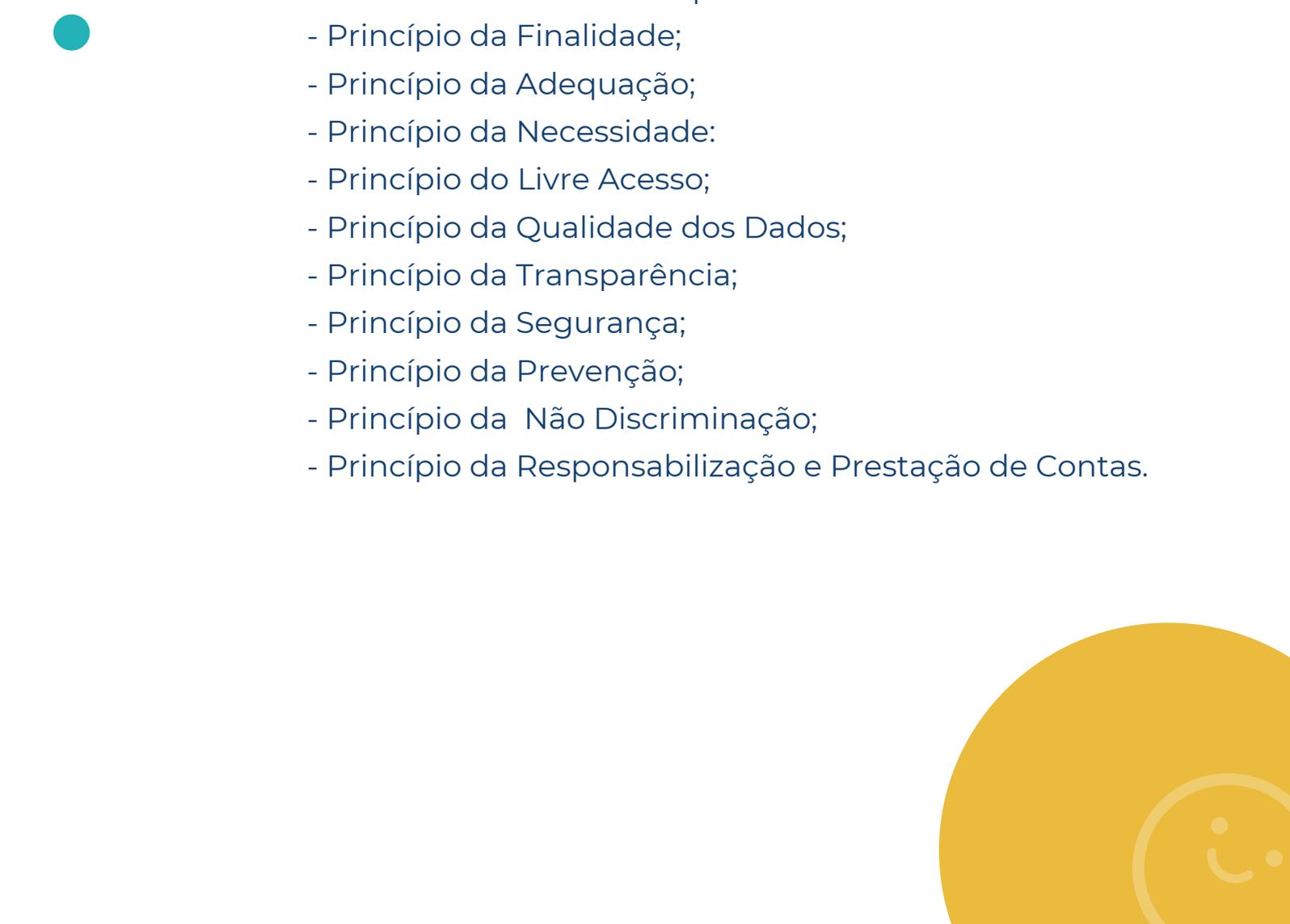
DPO (Data Protection Officer) ou Encarregado de Proteção de Dados Pessoais é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação aos titulares dos dados, ANPD e demais autoridades.





Quais são os princípios da LGPD?

A Lei Geral de Proteção de Dados apresenta alguns princípios que devem ser atendidos quando da realização do tratamento de dados pessoais:

- Princípio da Finalidade;
 - Princípio da Adequação;
 - Princípio da Necessidade;
 - Princípio do Livre Acesso;
 - Princípio da Qualidade dos Dados;
 - Princípio da Transparência;
 - Princípio da Segurança;
 - Princípio da Prevenção;
 - Princípio da Não Discriminação;
 - Princípio da Responsabilização e Prestação de Contas.
- 



Quais são as bases legais da LGPD?

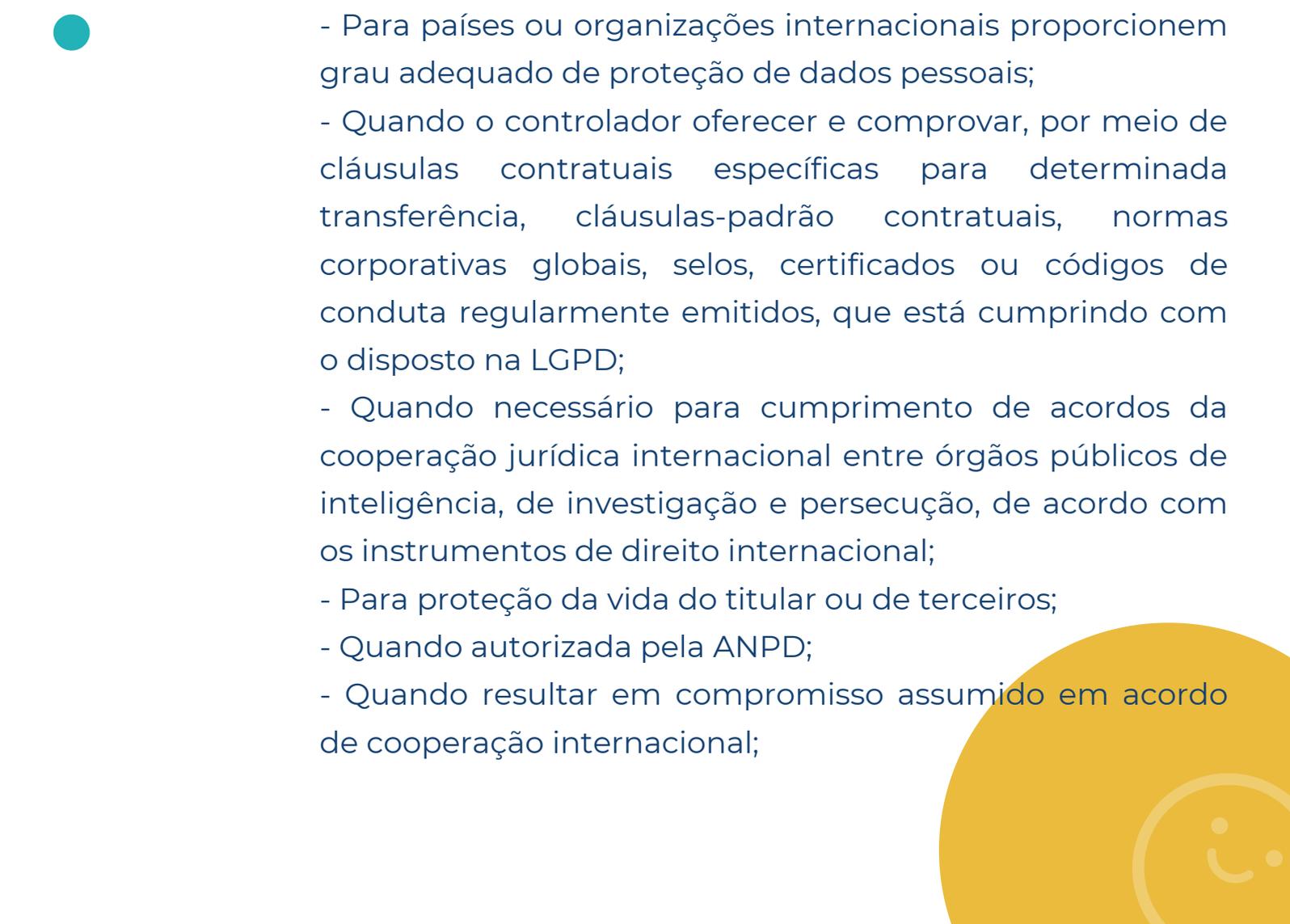
As bases legais são as hipóteses que legitimam as operações de tratamento de dados pessoais que o controlador realiza. Assim, este tratamento só poderá ser realizado:

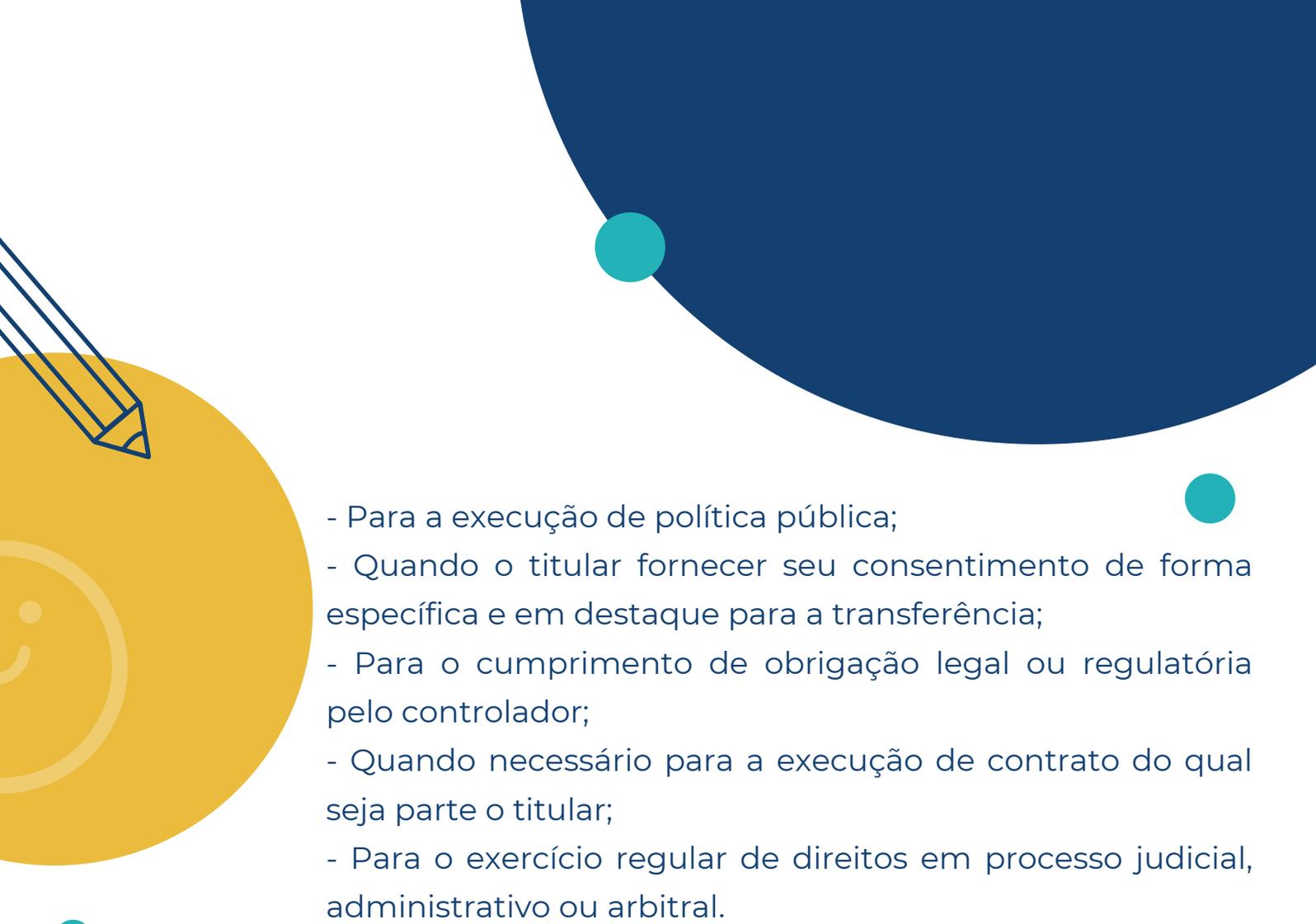
- Com consentimento do titular;
- Para cumprimento de obrigação legal ou regulatória;
- Pela Administração Pública;
- Para realização de estudos por órgãos de pesquisa;
- Para execução de contratos, a pedido do titular;
- Em processos judiciais, administrativos ou arbitrais;
- Para proteção da vida;
- Para tutela da saúde;
- Para atender o legítimo interesse do Controlador ou de terceiros;
- Para proteção do crédito.



Em quais hipóteses os dados pessoais podem ser transferidos para fora do Brasil?

A transferência internacional de dados pessoais pode ser feita:

- Para países ou organizações internacionais proporcionem grau adequado de proteção de dados pessoais;
 - Quando o controlador oferecer e comprovar, por meio de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados ou códigos de conduta regularmente emitidos, que está cumprindo com o disposto na LGPD;
 - Quando necessário para cumprimento de acordos da cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e persecução, de acordo com os instrumentos de direito internacional;
 - Para proteção da vida do titular ou de terceiros;
 - Quando autorizada pela ANPD;
 - Quando resultar em compromisso assumido em acordo de cooperação internacional;
- 

- 
- Para a execução de política pública;
 - Quando o titular fornecer seu consentimento de forma específica e em destaque para a transferência;
 - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
 - Quando necessário para a execução de contrato do qual seja parte o titular;
 - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Quais são as sanções previstas na LGPD?

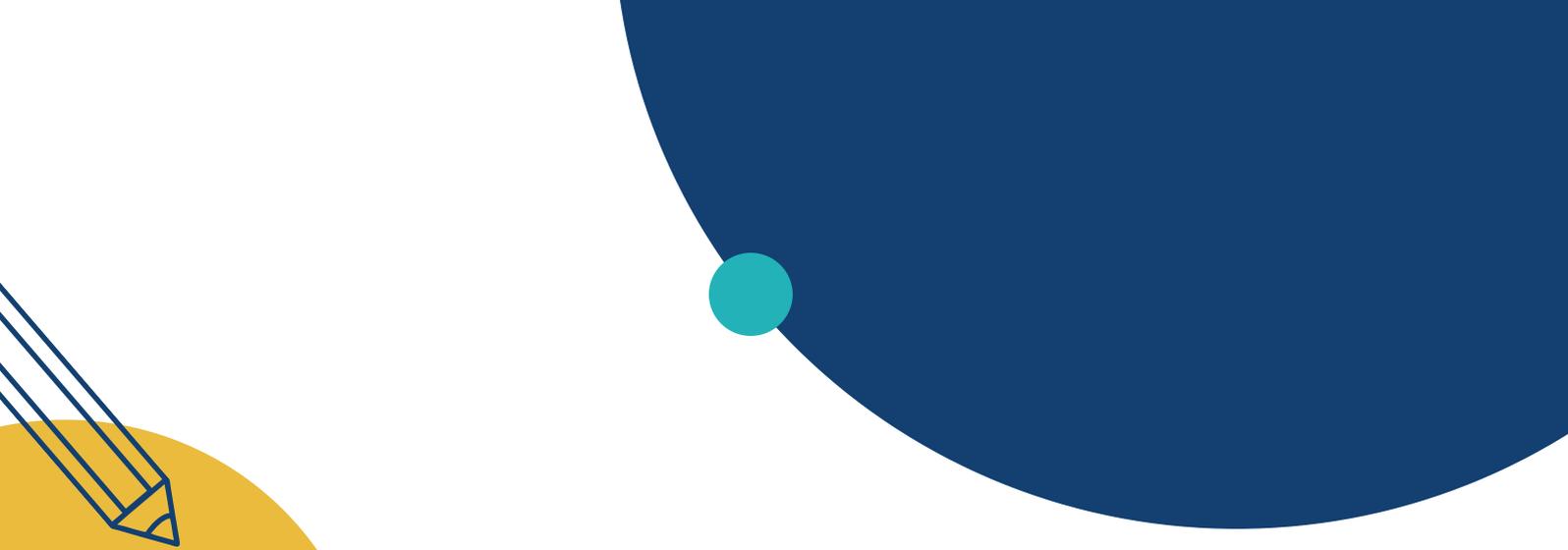
Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;





IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

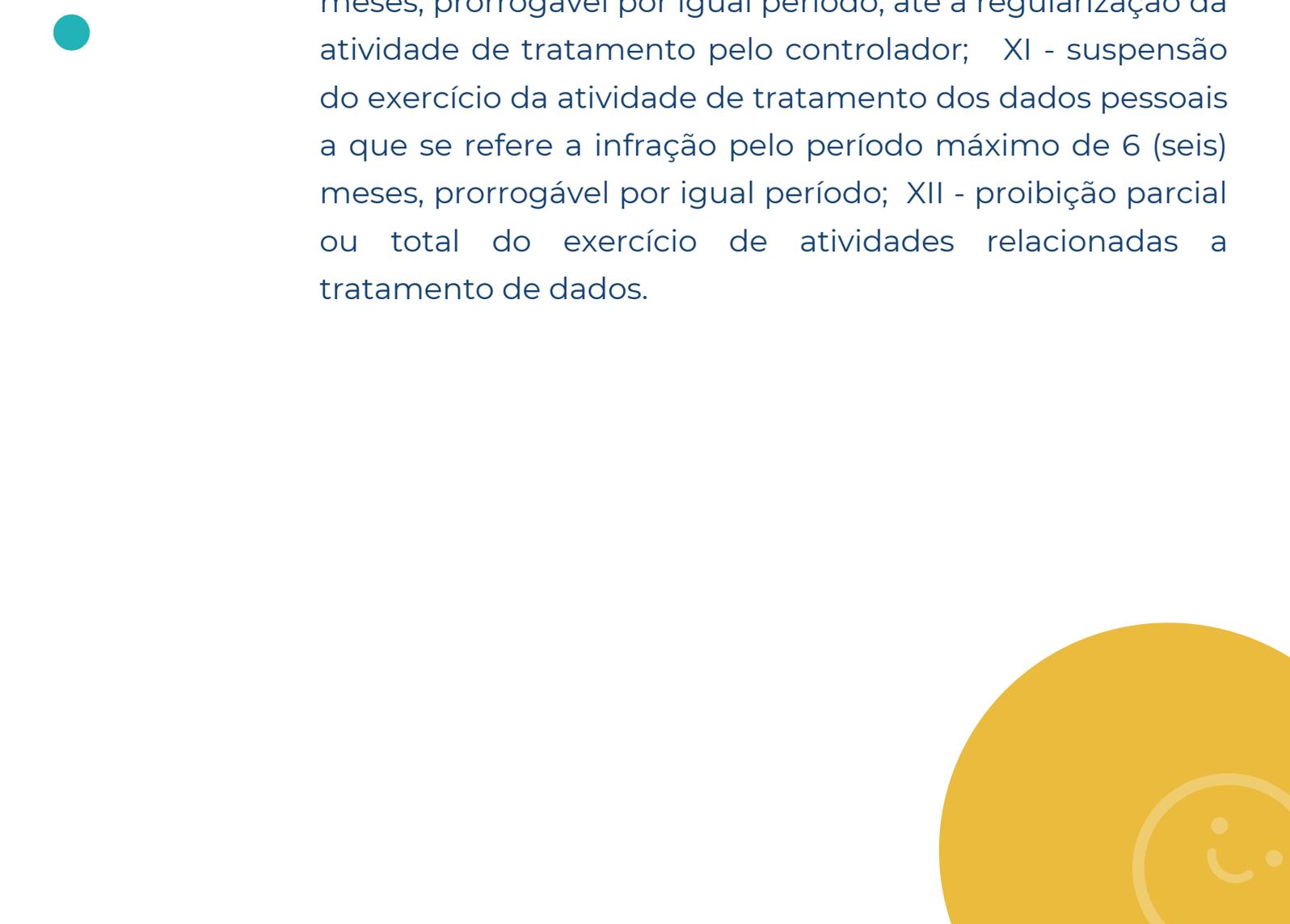
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

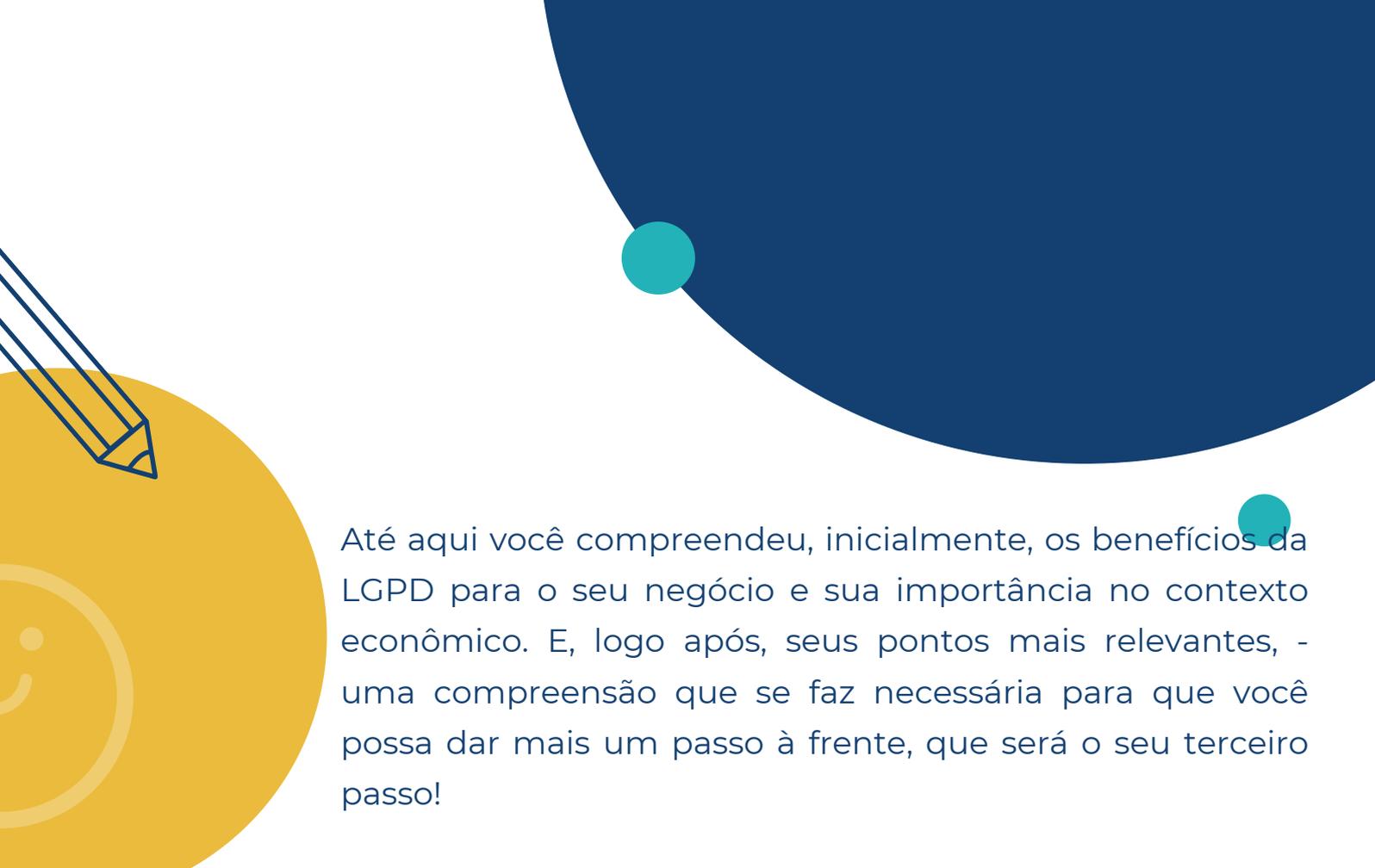
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.



Quais são os direitos dos titulares?

- I - confirmação da existência de tratamento;
- II - acesso aos dados;
- III - correção de dados incompletos, inexatos ou desatualizados;
- IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.



Até aqui você compreendeu, inicialmente, os benefícios da LGPD para o seu negócio e sua importância no contexto econômico. E, logo após, seus pontos mais relevantes, - uma compreensão que se faz necessária para que você possa dar mais um passo à frente, que será o seu terceiro passo!

Por onde começar a adequação da sua empresa? O que você precisa fazer primeiro? Qual o passo a passo?

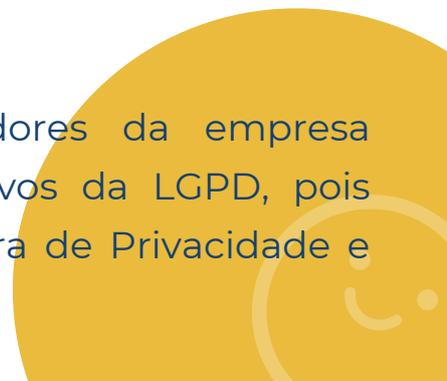
Passo 1: Conhecer e entender a Lei Geral de Proteção de Dados!

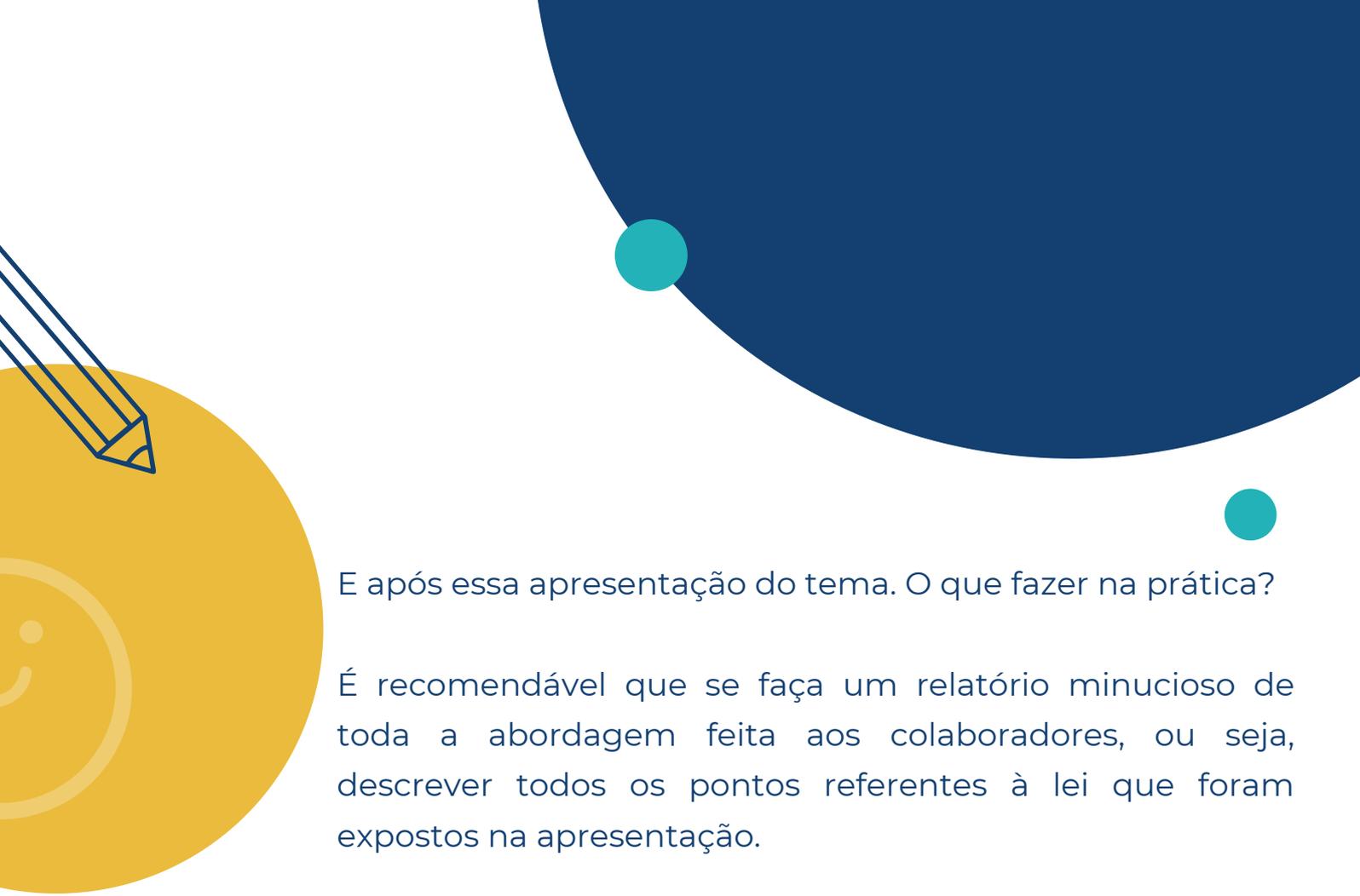
O primeiro e mais importante passo a ser dado rumo à jornada de adequação da sua empresa é a apresentação do tema para os colaboradores.

E como fazer isto?

Apresentando os principais aspectos e impactos da LGPD para todos os colaboradores que realizam suas atividades com base no tratamento de dados.

O ideal é que todos os colaboradores da empresa conheçam e compreendam os objetivos da LGPD, pois assim já estará se construindo a cultura de Privacidade e Proteção de Dados dentro da empresa.





E após essa apresentação do tema. O que fazer na prática?

É recomendável que se faça um relatório minucioso de toda a abordagem feita aos colaboradores, ou seja, descrever todos os pontos referentes à lei que foram expostos na apresentação.



Esse documento deverá ser datado e assinado por todos os presentes. E por que isso? Porque não basta só estar em conformidade ou buscando ela, é necessário que a empresa demonstre o seu comprometimento com a conformidade.

Além deste documento que constará no acervo de Políticas Internas, é super importante que a empresa publique em seus canais de comunicação com os clientes, o início da sua jornada rumo à conformidade e de forma a demonstrar a sua preocupação com a privacidade e a proteção de dados.

Passo 2: Assessment LGPD!

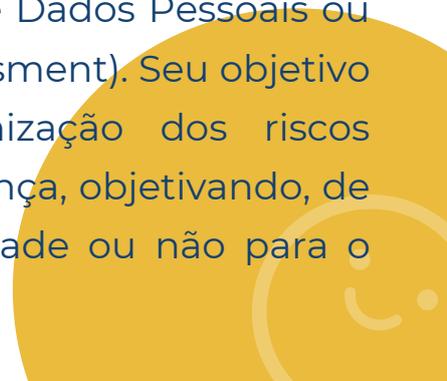
O Assessment nada mais é do que a avaliação inicial que objetiva o diagnóstico do cenário atual da empresa em relação à conformidade com a lei.

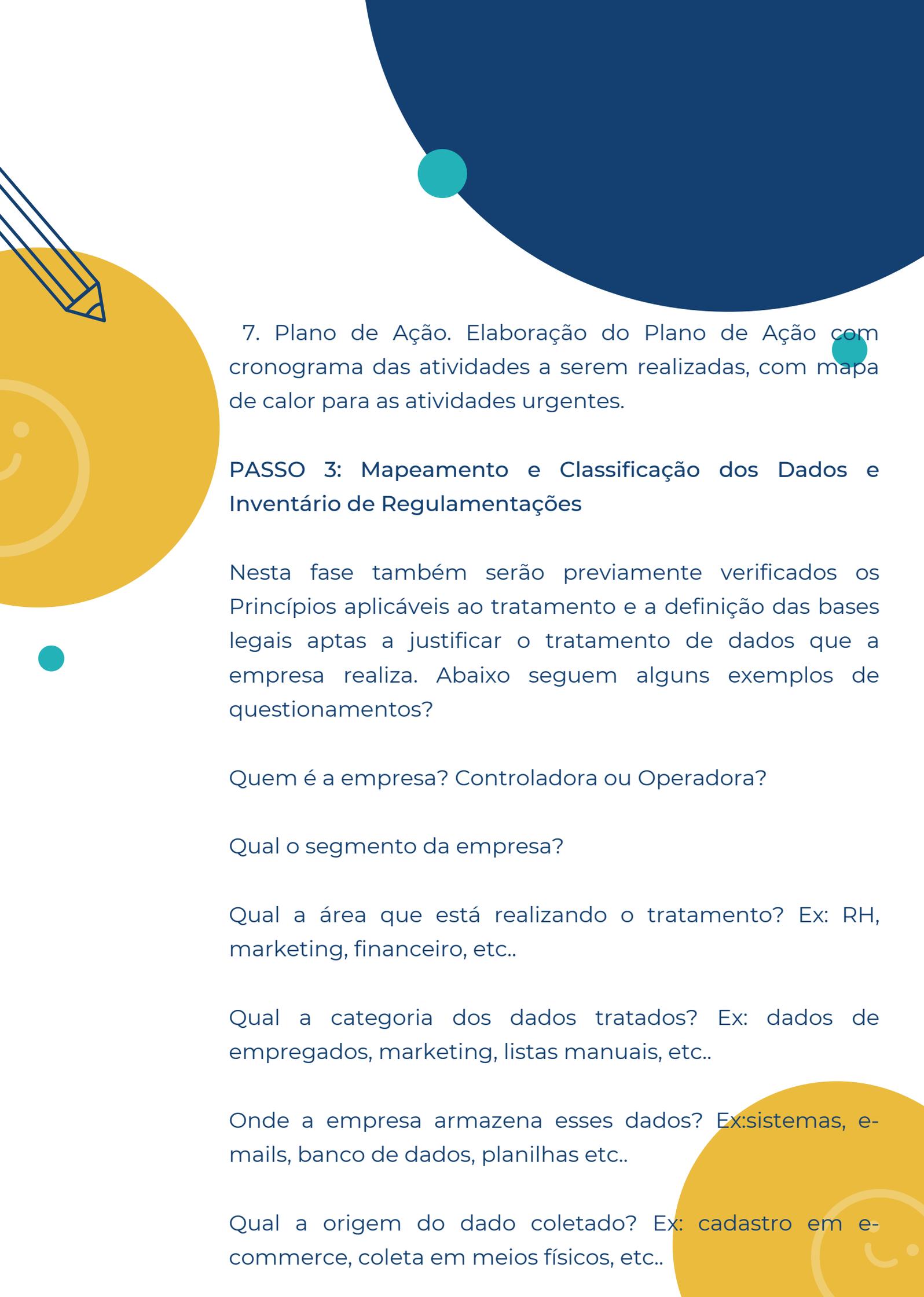




Neste momento é hora de verificar quais os requisitos da LGPD e demais legislações pertinentes ao seu negócio a empresa atende ou não. Por meio desta avaliação é que será possível compreender a maturidade dos processos, a adesão e a estratégia adotada pela empresa na busca pela conformidade.

E quais são as atividade realizadas neste segundo passo?

1. Criação do Comitê Multidisciplinar (time que atuará na realização das atividades iniciais).
 2. Mapeamento Inicial dos Dados (por áreas e por processos).
 3. LIA (Legitimate Interests Assessment) - Caso haja a opção do Legítimo Interesse para fundamentar o tratamento de dados que a empresa realiza.
 4. Mapa de Fluxo de Dados para compreender por onde o dado transita dentro da empresa.
 5. Elaboração do Relatório de Diagnóstico para fins de análise dos GAP's (brechas) encontradas.
 6. Relatório de Impacto à Proteção de Dados Pessoais ou DPIA (Data Protection Impact Assessment). Seu objetivo é análise, identificação e minimização dos riscos relacionados à incidentes de segurança, objetivando, de igual forma, a indicação da viabilidade ou não para o tratamento de dados pretendido.
- 



7. Plano de Ação. Elaboração do Plano de Ação com cronograma das atividades a serem realizadas, com mapa de calor para as atividades urgentes.

PASSO 3: Mapeamento e Classificação dos Dados e Inventário de Regulamentações

Nesta fase também serão previamente verificados os Princípios aplicáveis ao tratamento e a definição das bases legais aptas a justificar o tratamento de dados que a empresa realiza. Abaixo seguem alguns exemplos de questionamentos?

Quem é a empresa? Controladora ou Operadora?

Qual o segmento da empresa?

Qual a área que está realizando o tratamento? Ex: RH, marketing, financeiro, etc..

Qual a categoria dos dados tratados? Ex: dados de empregados, marketing, listas manuais, etc..

Onde a empresa armazena esses dados? Ex: sistemas, e-mails, banco de dados, planilhas etc..

Qual a origem do dado coletado? Ex: cadastro em e-commerce, coleta em meios físicos, etc..



Qual a finalidade da coleta?

Neste contexto de mapeamento, sugere-se que, após mapear todos os dados e realizar o inventário das regulamentações, deverá se verificar se o tratamento atende aos princípios da LGPD e quais as bases legais adequadas ao tratamento de dados realizado.

Passo 4: Implementação do Programa de Governança de Privacidade e Proteção de Dados!

Implementação prática pelo departamento jurídico!

Desenvolvimento do Programa de Governança de Privacidade e Proteção de Dados com estabelecimento de Políticas internas, revisão de Política de Privacidade, revisão de contratos, termos, etc..

Implementação prática pela área de Tecnologia da Informação!

Adoção das medidas técnicas pela área de TI a fim de atender ao disposto no art. 18 da LGPD.





Implementação dos controles de Segurança da Informação!

Execução das principais medidas de Segurança da Informação.

Passo 5: Boas Práticas!

Manual de Boas Práticas constando as Políticas Internas da empresa sobre Privacidade e Proteção de Dados, bem como o Código de Conduta sobre a forma como a empresa em geral se comportará em relação à Privacidade e Proteção de Dados, o modo como os colaboradores deverão agir neste contexto.

Passo 6: Manutenção do Programa de Governança!

Realização da manutenção da cultura de Privacidade e Proteção de Dados, para fins de treinamento e conscientização dos colaboradores acerca da importância de manter a privacidade e a proteção de dados.

Passo 7: Monitoramento do Programa de Governança!

- Revisão do Plano de Ação elaborado no *Assessment*;
- Realização de testes de validação e confiança do Programa;
- Avaliações periódicas.



Lembre-se: não importa o seu ramo de atuação, se em meios digitais ou físicos. Se a sua empresa realiza atividades por meio de operações de tratamento de dados, ela precisa estar em conformidade com a LGPD.

Você gostou deste conteúdo? Ele te ajudou? Então compartilhe ele com todas as pessoas que você entende que também precisam dele.



E se você deseja aprender cada detalhe da implementação de forma minuciosa, fique de olho no nosso site:

www.implementandoalgpd.com.br.

Em breve lançaremos o nosso curso, onde você terá a oportunidade de aprender a adequar a sua empresa na prática.

Caso tenha alguma dúvida, terei o maior prazer em ajudá-lo(a).

contato@implementandoalgpd.com.br

Contem comigo!

Um grande abraço,

Jerusa Bohrer

