MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 1 /2021

NOME DA INSTITUIÇÃO: Centre for Information Policy Leadership (CIPL)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, conforme disposto no art. 55-J, XVIII, da LGPD e item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões com abordagem gerais, como a identificação dos principais problemas regulatórios que devem ser tratados na regulamentação e mapeamento de experiências internacionais que tratem do tema, e questões específicas, como a definição de microempresa e de empresa de pequeno porte que seja mais adequada para a regulação setorial de proteção e privacidade de dados, o impacto que as regras dispostas na LGPD podem causar aos agentes de pequeno porte (manutenção do registro das operações de tratamento de dados pessoais, elaboração de relatório de impacto à proteção de dados pessoais, tratamento de dados em conformidade com a legislação, indicação do encarregado de tratamento de dados pessoais, portabilidade de dados dos titulares e garantia de segurança, boas práticas e governança dos dados pessoais), bem como alternativas regulatórias para incentivar e promover a inovação nestes agentes.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

SOBRE O CIPL

O Centre for Information Policy Leadership (CIPL) recebe com satisfação a oportunidade de responder à primeira consulta pública organizada pela Autoridade Nacional de Proteção de Dados (ANPD) e gostaria de elogiar a ANPD por buscar cooperação e contribuições de múltiplas partes interessadas.

O CIPL é um think tank global que atua na área de privacidade e proteção de dados e segurança da informação com sede em Washington D.C., Londres e Bruxelas, fundado em 2001 no escritório de advocacia Hunton Andrews Kurth LLP. A missão do CIPL é se engajar em liderança de ideias e promover boas práticas que

garantam tanto a proteção efetiva da privacidade quanto o uso responsável dos dados pessoais na era moderna da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e tomadores de decisão em todo o mundo. Trabalhamos com líderes seniores e especialistas em privacidade de mais de 75 organizações globais líderes que nos fornecem casos concretos sobre suas práticas de privacidade de dados e tomada de decisões. Veja mais sobre o CIPL em https://www.informationpolicycentre.com/.

Nada nesta apresentação deve ser interpretado como representando a opinião individual de qualquer empresa membro do CIPL ou do escritório de advocacia Hunton Andrews Kurth.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quais são os desafios/problemas regulatórios relacionados ao tema?	A Lei Geral de Proteção de Dados (LGPD) prevê que a ANPD deve elaborar regras específicas relativas ao cumprimento desta lei pelas pequenas e médias empresas (PMEs) (Artigo 55-J, XVIII). O CIPL entende que muitas organizações e associações industriais têm defendido que as PMEs sejam isentas de uma série de disposições da LGPD. Embora as isenções possam ser apropriadas em alguns casos, **a Autoridade Nacional de Proteção de Dados (ANPD) deve (i) ser flexível e razoável, seguindo a natureza da abordagem baseada em risco da LGPD ao elaborar regras que possam isentar as PMEs das disposições da LGPD, e (ii) focar nos melhores resultados para os indivíduos e a sociedade, levando em conta os vários desafios e riscos que se relacionam com este tópico, descritos abaixo**: • Devido à LGPD ser a primeira lei abrangente de proteção de dados no Brasil, existe geralmente uma falta de conscientização e um nível de maturidade baixo sobre este tópico, inclusive entre as PMEs; • A LGPD entrou em vigor no meio da pandemia da COVID-19. Enquanto a COVID-19 representou oportunidades para alguns setores industriais e organizações maiores, muitas PMEs foram fortemente impactadas e tiveram que direcionar seus já escassos recursos para sobreviver à crise em vez de cumprir com as novas regras de proteção de dados. Há preocupações de que muitas serão incapazes de retomar seus negócios após a crise;

	• A ausência de clareza quanto ao escopo de aplicabilidade da LGPD às PMEs leva a que estas (i) incorram em custos de conformidade desnecessários que podem não ser proporcionais à natureza dos riscos das suas atividades de tratamento de dados para os titulares dos dados ou (ii) se abstenham de cumprir com as regras da LGPD em geral; • A não conformidade com a LGPD, em particular entre as PMEs, o que pode acarretar o risco de tornar a LGPD ineficaz e consequentemente diminuir o nível de proteção para os brasileiros. Isto pode resultar em um efeito dominó no qual organizações privadas maiores, bem como organizações do setor público, podem não levar a sério as regras da LGPD. Em última instância, isso dificultará o desenvolvimento da economia digital e da inovação, e impedirá o desenvolvimento de uma cultura de proteção de dados no Brasil. Uma falta geral de conformidade e eficácia da LGPD pode ter um impacto negativo em futuras decisões de adequação ou acordos bilaterais para fins de transferência internacional de dados entre o Brasil e outros países; • A falta de conformidade das PMEs com a LGPD (e em particular daquelas PMEs que têm um modelo de negócios baseado em dados) corre o risco de criar uma lacuna de conformidade na cadeia de comércio do mundo digital que pode de fato excluí-las de outras oportunidades de negócios e desenvolvimento. Este poderia ser o caso se as PMEs não cumprirem com as regras da LGPD ou se lhes forem concedidas demasiadas isenções de conformidade. Um membro do CIPL, que é uma organização internacional, relatou que em alguns casos se abstem de entrar em contratos com PMEs brasileiras, uma vez que elas muitas vezes são incapazes de cumprir com suas exigências relacionadas à segurança da informação que são requeridas por leis de outras jurisdições. Além disso, alguns membros do CIPL relataram que podem considerar não se envolver com as PMEs brasileiras como fornecedores/processadores/parceiros de negócios se as isenções a serem fornecidas pela ANPD levarem as PMEs a não protegerem efetivamente os dados pessoais conforme apropriado aos riscos de suas atividades de tratamento de dados, uma vez que isto pode afetar a conformidade geral desses membros do CIPL; • Portanto, o principal desafio da ANPD tem dois aspectos: (i) oferecer às PMEs regras que sejam flexíveis, escaláveis e que permitam sua conformidade com as regras da LGPD, incentivndo-as a se tornarem responsáveis em relação aos dados pessoais e permitindo seu funcionamento em uma economia brasileira impulsionada por dados após a COVID-19 e (ii) evitar que isenções excessivas às regras de conformidade e aplicação levem as PMEs a não cumprir com outras regras aplicáveis da LGPD, conforme apropriado ao risco de suas atividades de tratamento de dados, além de não temer possíveis sanções pela ANPD.

	Veja como referência os seguintes documentos do CIPL: • Looking Beyond COVID-19: Future Impacts on Data Protection and the Role of the Data Protection Authorities (2 de junho de 2020) • The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (23 de julho de 2018) – para obter mais informações sobre o impacto da responsabilização nas disposições contratuais e nas negociações dentro das cadeias de comércio
Existem sugestões para endereçamento do problema?	Há uma série de medidas que a ANPD pode tomar para enfrentar os desafios e riscos descritos acima de uma maneira baseada em riscos (*risk-based*) e em resultados (*outcomes-based*): • **Fornecer orientação às PMEs** – A ANPD deve priorizar o fornecimento de orientação às PMEs para esclarecer as muitas disposições da LGPD aplicáveis. Além disso, a ANPD deve ajudá-las a entender a importância de proteger os dados pessoais e tornarem-se responsáveis. ○ Essas orientações devem se concentrar não apenas (i) nas urgentes disposições da LGPD (por exemplo, exigências relativas às informações a serem fornecidas sobre o tratamento de dados e à transparência, nomeação de um encarregado, realização de uma relatórios de impacto, manutenção de registros das atividades de tratamento, etc.), mas também (ii) em temas de proteção de dados que são fundamentais para a utilização de dados pessoais pelas PMEs para inovação (por exemplo, compartilhamento de dados, interesses legítimos, pseudonimização e anonimização, treinamento algorítmico com base em dados, transferências internacionais de dados, etc.); ○ A ANPD deve trabalhar com associações industriais para identificar quais são os tópicos mais urgentes para as PMEs; ○ Qualquer orientação fornecida pela ANPD às PMEs deve ser escrita em linguagem simples e clara (em oposição à linguagem legalista), ser concisa e pragmática (ou seja, abordar as necessidades operacionais práticas das PMEs); ○ Há muitas maneiras pelas quais a ANPD poderia fornecer tais orientações, como através de diretrizes formais, uma página no site da ANPD dedicada às PMEs reunindo recursos relevantes, perguntas frequentes, documentos curtos e simplificados (por exemplo, de uma página com elementos visuais), estudos de caso, exemplos concretos das práticas recomendadas, documentos mostrando o que fazer e o que não fazer, mostrando o que é bom e ruim, etc. (veja nossa resposta às perguntas "Quais são as experiências internacionais relacionadas a este

	tópico?" e "Como a UE abordou a conformidade com a Regulamento Geral sobre a Proteção de Dados (GDPR) pelas PMEs?" para obter exemplos do que outros reguladores de proteção de dados estão fazendo para fornecer orientações às PMEs); • **Desenvolver e promover ferramentas e modelos de accountability e e de conformidade à LGPD para PMEs** – incluindo modelos (como para registros de tratamento, relatórios de impacto, avaliações de interesses legítimos), questionários automatizados, listas de verificação (*checklists*) (como para os componentes principais de um programa de governança de dados), ferramentas de autoavaliação e outros. No entanto, a ANPD deve deixar claro que tais ferramentas e modelos são indicativos e não obrigatórios, e que as PMEs, bem como as organizações maiores, devem ser livres para usar quaisquer outras ferramentas e modelos que considerem mais adequados para alcançar os resultados de proteção de dados buscados; • **Incentivar o desenvolvimento de códigos de conduta do setor** – veja abaixo a resposta à pergunta: "Quais mecanismos regulatórios poderiam ser usados para promover e incentivar a inovação pelas PMEs?"; • **Possibilitar o desenvolvimento de certificações, selos e marcas** – uma vez que eles têm potencial para desempenhar um papel significativo em permitir que as organizações, em particular as PMEs, alcancem e demonstrem accountability organizacional e, portanto, se coloquem em uma melhor posição competitiva; • **Incentivar o compartilhamento de boas práticas de proteção, gerenciamento e "higiene de dados" entre organizações profissionais brasileiras** – através de iniciativas do setor como mesas redondas, análise comparativa à outras organizações (*benchmarking*), criação de redes de encarregados pelo tratamento de dados, publicação de modelos e metodologias utilizados por setores específicos de indústria, reconhecimento de modelos de accountability, tais como o CIPL Accountability Framework (ver figura abaixo) para o desenvolvimento de programas de governança de dados, e aumentando a conscientização dos benefícios da accountability (ver o Estudo de Benchmark de Privacidade de Dados 2021 da Cisco). Em particular, a ANPD deveria incentivar organizações maiores e mais maduras a compartilhar suas boas práticas e ferramentas com as PMEs (por exemplo, empresas tecnológicas maiores que apoiam a conformidade LGPD de terceiros através do compartilhamento de informações e boas práticas), uma vez que isso ajudaria a melhorar a conformidade e a responsabilização em todo o ecossistema de dados. As organizações maiores e mais maduras têm um papel fundamental a desempenhar na implementação da accountability através da cadeia de fornecedores/vendedores;

	• **Conduzir programas de educação e conscientização voltados para as PMEs**;
	• **Proporcionar oportunidades para que as PMEs se envolvam e compartilhem com a ANPD sua experiência de conformidade** – por exemplo, através de mesas redondas, sandboxes (veja abaixo nossa resposta à pergunta: "Quais mecanismos regulatórios poderiam ser usados para promover e incentivar a inovação pelas PMEs?"), questionários, pesquisas, etc.;
	• **Levar em consideração, quando executar a LGPD, os esforços relacionados à responsabilização organizacional (accountability) tomados pelas PMEs (assim como outras organizações), e incluir a previsão de tais considerações no futuro regulamento sobre sanções administrativas a infrações à LGPD** – isto incentivará as PMEs, bem como as organizações maiores, a implementar o princípio da responsabilização e prestação de contas, o que resultará em um aumento da confiança no ecossistema de dados (veja explicação abaixo);
	• **Possibilitar transferências internacionais de dados pessoais, permitindo assim que as PMEs brasileiras participem da economia digital global** – através do:
	  ○ Desenvolvimento de mecanismos de transferência de dados e orientações relativas a esses mecanismos (por exemplo, cláusulas contratuais padrão, normas corporativas globais, códigos de conduta, certificações, selos e marcas);
	  ○ Incentivo à adesão do Brasil a esquemas regulatórios de transferência de dados, tais como o Cross-Border Privacy Rules (CBPR) da Cooperação Econômica da Ásia-Pacífico (APEC) quando este se abrir para países fora da APEC;
	  ○ Reconhecimento de certificações internacionais, tais como certificações ISO e de normas corporativas globais obtidas sob outros regimes de proteção de dados como mecanismos válidos de transferência de dados;
	  ○ Incentivo à negociação de acordos bilaterais de transferência de dados entre o Brasil e outros países;
	• **Trabalhar com autoridades públicas de outras áreas regulamentadas, bem como associações de indústria para identificar iniciativas intersetoriais para apoiar o cumprimento da LGPD pelas PMEs** – outras leis brasileiras também se aplicam às PMEs no âmbito de suas operações de tratamento de dados. Logo, as PMEs se beneficiariam de atividades de

	conscientização e outras iniciativas para facilitar seu entendimento das diversas regras do cenário jurídico brasileiro (por exemplo, sandboxes, mesas redondas, diretrizes elaboradas conjuntamente entre diversos reguladores); e • **Em particular, ao fornecer diretrizes e ferramentas às PMEs, a ANPD deve dar prioridade à promoção do princípio da responsabilização e prestação de contas (accountability) como facilitador da proteção efetiva dos dados pessoais e do uso responsável de tais dados, e promover a accountability como a base para o cumprimento da LGPD.** O princípio da accountability está emergindo nas leis de proteção de dados ao redor do mundo assim como em outras áreas reguladas (como concorrência, combate à fraude, anticorrupção e outras). Isto permitirá com que as PMEs utilizem seus esforços de conformidade com a LGPD para conformidade com essas outras áreas reguladas e vice-versa. A accountability é reconhecida mundialmente como um elemento-chave para a regulamentação eficaz da privacidade e proteção de dados pessoais. Desde a inclusão do princípio de accountability nas Diretrizes da OCDE sobre Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais em 1980, ele tem sido reconhecido em muitas leis e e modelos de proteção de dados como um princípio fundamental. Accountability significa que as organizações: • Adotam medidas para converter os requisitos legais de privacidade de dados em ações e controles baseados em riscos, concretos, verificáveis e aplicáveis ao tratamento de dados pessoais, que são revisados e adaptados ao longo do tempo – tais medidas incluem a implementação de um programa de governança de dados; e • São capazes de demonstrar a existência e eficácia de programas de governança de dados internamente (por exemplo, para a diretoria e a alta administração) e externamente (por exemplo, para as autoridades de proteção de dados, indivíduos, parceiros comerciais e acionistas). Há anos o CIPL trabalha extensivamente em accountability e defende a aceitação e implementação desse princípio por organizações de todos os tamanhos e órgãos reguladores de privacidade e proteção de dados em todo o mundo. Em 2020, o CIPL concluiu um projeto chamado Accountability Mapping Project, onde analisamos e mapeamos práticas reais de prestação de contas empreendidas por 17 organizações de vários setores da indústria, tamanhos e regiões, incluindo duas PMEs e uma universidade. Isto levou à identificação de uma série de tendências, inclusive que **a accountability é um conceito escalável e agnóstico em relação a setores de indústria. Ou seja, organizações de todos os tipos, tamanhos, setores (incluindo o setor público), presenças geográficas e culturas corporativas podem desenvolver e implementar programas de governança de dados e outras medidas de accountability, até mesmo as PMEs.** O programa, as atividades específicas (políticas, procedimentos, controles e ferramentas) e os recursos humanos e financeiros serão diferentes em cada organização, apropriados ao seu contexto

	específico, riscos, metas e tamanho. Em particular, enquanto as organizações menores podem e tomam medidas para serem responsáveis, elas calibram essas medidas de maneira diferente (e muitas vezes mais agilmente) em relação às organizações maiores, multinacionais. Independente, a arquitetura geral de accountability adotada por essas organizações pode ser a mesma, como sugerido pelo CIPL Accountability Framework. **A ANPD deve incentivar organizações de todos os tamanhos a serem responsáveis e deve promover o uso de modelos de accontability como o CIPL Accountability Framework (ver figura abaixo) para que as PMEs e organizações maiores estruturem seus programas de governança de dados**. O CIPL Accountability Framework é uma arquitetura ideal e bem estabelecida para construir e organizar um programa eficaz de governança de dados que converta os requisitos legais da LGPD e de outras leis de proteção de dados em controles acionáveis. Ele também permite que as organizações sejam sistemáticas, que avaliem seu programa de governança de dados e sua jornada de prestação de contas com o tempo e tomem medidas para melhorar e adaptar a proteção de dados.  *Figura: a CIPL Accountability Framework*

	Veja como referência os seguintes documentos do CIPL e outros recursos sobre o princípio da accountability: • Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD) (1 de setembro de 2020) • What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework (27 de maio de 2020) • The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (23 de julho de 2018) • Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability (23 de julho de 2018) • Organisational Accountability - Past, Present and Future (30 de outubro de 2019) • Em maio de 2020, durante o discurso de abertura da conferência da Privacy + Security Academy, a Comissária da FTC, Christine Wilson, apresentou a accountability como boa prática de privacidade que é particularmente relevante para o desenvolvimento de programas de governança de dados, citando o CIPL Accountability Framework como exemplo. Ela explicou os sete elementos da CIPL Accountability Framework e recomendou que as empresas avaliaem seus programas de governança de dados à luz desses elementos. Veja como referência os seguintes documentos do CIPL sobre a regulamentação efetiva: • The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD) (16 April 2020) • Regulamentando para Gerar Resultados – Estratégias e Prioridades para Liderança e Engajamento (25 de setembro de 2017, atualizado em 10 de outubro de 2017)) Veja outros documentos do CIPL: • Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy (25 de setembro de 2017) • CIPL Q&A on Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) (19 de março de 2020) • Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms (12 de abril de 2017)

Quais são as oportunidades relacionadas ao tema?	Há uma série de oportunidades para a ANPD no contexto das regras sobre PMEs: • O foco da LGPD é de proteção dos direitos e liberdades dos indivíduos. A LGPD reconhece que todas as partes envolvidas no ecossistema de tratamento de dados pessoais têm algum nível de accountability para garantir que esses direitos e liberdades sejam protegidos, incluindo as PMEs. **A ANPD tem uma oportunidade de incentivar que a accountability seja implementada em todo esse ecossistema de dados/cadeia de comércio digital, que é cada vez mais complexo** e inclui controladores, processadores e subprocessadores dentro e fora das fronteiras brasileiras. Isto apoiará a construção de uma cultura de proteção de dados no Brasil, assim como promoverá o desenvolvimento econômico digital e a inovação; • **A ANPD tem a oportunidade de se posicionar como uma autoridade líder e visionária** no Brasil (em relação às autoridades de outras áreas reguladas, como consumidor e concorrência) e fora do Brasil (em relação a outros reguladores de proteção de dados, em particular da América Latina); e • **A ANPD tem a oportunidade de ser vista como um regulador construtivo** que está aberto ao engajamento com organizações reguladas, incluindo PMEs, e obter informações e feedback das mesmas a fim de gerar diretrizes pragmáticas e eficazes.
Quais são as experiências internacionais sobre o tema?	Muitos reguladores de privacidade e proteção de dados em todo o mundo emitiram orientações e ferramentas para apoiar PMEs a entrarem em conformidade com leis de privacidade e proteção de dados pessoais. Seguem abaixo links para tais orientações e ferramentas fornecidas por reguladores que o CIPL acretira serem visionários e que seguem uma abordagem baseada em risco e geração de resultados (*risk-based approach* e *outcomes-based approach*): • O **UK Information Commissioners' Office (UK ICO)** tem uma página web dedicada às PMEs, diretrizes curtas direcionadas às PMEs chamadas de "Getting it right: a brief guide to data protection for small businesses" e o ICO Accountability Framework; • A **US Federal Trade Commission (FTC)** também tem uma página web dedicada a oferecer orientação a todas as pequenas empresas; • Da mesma forma, o **Office of the Privacy Commissioner of Canada (OPC)** tem uma página web com dicas e ferramentas para ajudar pequenas empresas a lidar com privacidade;

	• O **Singapore Privacy Commissioner (Singapore PDPC)** oferece várias ferramentas para apoiar PMEs no início de sua jornada de conformidade com regras de proteção dos dados; • O **Hong Kong Privacy Commissioner (HK PDPC)** publicou três diretrizes para PMEs: (i) From Principles to Practice – SME Personal Data Protection Toolkit (junho de 2020), (ii) Data Ethics for Small and Medium Enterprises (abril de 2019) e (iii) Data Protection & Business Facilitation - Guiding Principles for Small and Medium Enterprises (dezembro de 2017); • O **Ireland Data Protection Commissioner (Irish DPC)** publicou uma diretriz para PMEs; • O **regulador de privacidade de dados de Guernsey (ODPA)** publicou em 2018 uma carta aberta pragmática às pequenas empresas e ONGs no contexto da reforma de proteção de dados de Guernsey, reconhecendo que as mudanças legais podem ter um impacto maior nas PMEs, que PMEs nem sempre têm os mesmos recursos ou habilidades à sua disposição comparadas a organizações maiores, e encaminhando PMEs para o centro de recursos do ODPA.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Esta pergunta parece cobrir dois conceitos distintos: (i) o conceito de PME e (ii) o conceito de controladores e operadores. Com relação (i) ao conceito de PMEs para fins de aplicação das regras da LGPD, há uma série de critérios que a ANPD poderia considerar, tais como número de funcionários, receita anual, volume de dados processados, tipos de atividades de tratamento de dados. Em qualquer caso, **a ANPD deve aplicar uma abordagem baseada em riscos às suas regras para PMEs e exigir que as organizações, independente do seu tamanho, implementem medidas técnicas e organizacionais mais robustas para proteger dados pessoais quando suas atividades de tratamento de dados representam riscos maiores para os indivíduos**. A ANPD deve fornecer orientações flexíveis e adaptáveis a mudanças futuras (*future-proof*) sobre avaliações de risco, bem como exemplos concretos de atividades de tratamento de dados que possam resultar em maiores riscos para os indivíduos (por exemplo, tratamento envolvendo dados pessoais sensíveis ou dados relativos a crianças, tratamento envolvendo novas tecnologias). A ANPD também deve deixar claro que qualquer avaliação de risco deve ser feita caso a caso, levando em conta todas as circunstâncias envolvidas. Com relação (ii) ao conceito de controladores e operadores, é importante que, para coerência e segurança jurídica, **os mesmos critérios da LGPD com relação à definição de controladores e operadores se apliquem a todas as organizações, independentemente de seu tamanho**. O artigo 5, VI e VII da LGPD define:

	• Controladores como "pessoa física ou jurídica de direito público ou privado encarregada de tomar as decisões relativas ao tratamento de dados pessoais"; e • Operadores como "pessoa física ou jurídica de direito público ou privado que processa dados pessoais em nome do controlador". Portanto, as PMEs que tomam decisões relativas ao tratamento de dados pessoais devem ser caracterizadas como controladoras e as PMEs que processam dados pessoais em nome das controladoras devem ser caracterizadas como operadoras. **A ANPD pode decidir, entretanto, esclarecer os conceitos/definições de controlador e operador sob a LGPD separadamente das regras relacionadas às PMEs e, ao fazê-lo, deve permanecer flexível e adaptável a mudanças futuras**. Veja como referência o seguinte documento do CIPL sobre as funções dos controladores e processadores (operadores) sob a GDPR: • CIPL Response to the EDPB's Guidelines on the Concept of Controller and Processor in the GDPR (19 de outubro de 2020)
Como a União Europeia tem atuado para que agentes de tratamento de dados de pequeno porte estejam em conformidade com a General Data Protection Regulation (GDPR)?	Em sua contribuição para a avaliação da GDPR nos termos do Artigo 97 (18 de fevereiro de 2020), o European Data Protection Board (EDPB) reconheceu que a implementação do GDPR tem sido um desafio, especialmente para pequenos atores como as PMEs. O EDPB está empenhado em facilitar o desenvolvimento de ferramentas por autoridades de proteção de dados da UE que aliviem a carga de conformidade de PMEs. **O EDPB enfatizou que, de qualquer forma, a abordagem baseada em risco da GDPR deve ser mantida, pois os riscos para os titulares dos dados não dependem do tamanho dos controladores e operadores** (observe, por exemplo, que as obrigações específicas da GDPR, tais como a nomeação de um encarregado e a realização de relatórios de impacto ou *DPIAs*, dependem de fatores de risco como a escala e a natureza do tratamento e não do tamanho da organização). Além disso, o EDPB incluiu uma extensa lista de orientações, ferramentas e iniciativas que as autoridades da UE disponibilizaram às PMEs (ver páginas 35-45 da contribuição do EDPB). O EDPB também incluiu ações específicas na sua Estratégia EDPB 2021-2023 (15 de dezembro de 2020) com o objetivo de facilitar a conformidade com a GDPR, inclusive pelas PMEs. Essas ações são: • Oferecer mais orientações sobre noções-chave de proteção de dados da UE através da organização de eventos dedicados às partes interessadas (incluindo grandes empresas e PMEs, ONGs, redes de encarregados e outros profissionais de proteção de dados) e de consultas públicas;

	• Promover ainda mais o desenvolvimento e a implementação de mecanismos de conformidade por controladores e operadores, em particular códigos de conduta e certificações, por exemplo, através de oficinas (*workshops*) e treinamento; e • Promover o desenvolvimento de ferramentas para um público mais amplo e envolver-se em atividades de conscientização e divulgação, em particular ferramentas especificamente adaptadas para profissionais não especializados, PMEs, e para os titulares dos dados. Além disso, o EU Commission multi-stakeholder expert group, o qual tem a atribuição de auxiliar a Comissão Europeia na identificação dos potenciais desafios na aplicação do GDPR e no aconselhamento sobre como enfrentá-los, também emitiu um relatório sobre a avaliação da GDPR sob o Artigo 97 (17 de junho de 2020). Esse grupo de especialistas identificou uma série de desafios relativos à aplicabilidade da GDPR pelas PMEs, incluindo: • As PMEs geralmente carecem dos recursos humanos e econômicos necessários para implementar as obrigações da GDPR, por isso se voltam para soluções padrão (instrumentos e modelos de conformidade mais fáceis) oferecidos tanto por associações como por empresas privadas; • As PMEs têm gasto recursos consideráveis para se adaptar às obrigações da GDPR, tais como documentação ou estabelecimento de políticas de tratamento de dados, e elas percebem isso como um aumento das obrigações administrativas; • Muitas PMEs tiveram que buscar assessoria de consultores externos para entender as regras da GDPR e entrar em conformidade; • Ainda não há um nível suficiente de entendimento por parte das PMEs sobre o conceito de consentimento livre e as consequências do tratamento de dados com base no "consentimento vinculado"; e • As PMEs relataram dificuldades na implementação de regras relativas à retenção de dados, medidas de segurança, transferências internacionais e tratamento de relatórios de impacto. O grupo de especialistas da Comissão Europeia também identificou uma série de mecanismos para apoiar as PMEs em seus esforços de conformidade com o GDPR: • Diretrizes concretas e ferramentas, tais como modelos, para ajudá-las a aplicar a GDPR na prática;

	• Cláusulas contratuais padrão para permitir transferências internacionais de dados pessoais, já que ao usá-las as PMEs não precisariam negociar contratos individuais; e • Códigos de conduta. Finalmente, a GDPR isenta organizações com menos de 250 funcionários de sua obrigação de manter registros de atividades de tratamento de dados, a menos que o tratamento (i) possa resultar em risco aos direitos e liberdades dos titulares dos dados, (ii) não seja ocasional, ou (iii) inclua dados sensíveis ou relativos a condenações e infrações penais (Artigo 30, 5, GDPR). Note que o objetivo do legislador da UE foi aliviar a carga de conformidade das PMEs e, ainda assim, ele aplicou uma abordagem baseada em risco a esta isenção. Na prática, porém, poucas organizações poderão contar com tal isenção, pois qualquer tratamento de dados pessoais pode implicar "um risco para os direitos e liberdades dos titulares dos dados". Este desafio também foi reconhecido pelo grupo de especialistas da Comissão Europeia no relatório mencionado acima. Veja como referência os seguintes documentos do CIPL: • GDPR One Year In - Practitioners Take Stock of the Benefits and Challenges (31 de maio de 2019) • CIPL Response to the EU Commission's Public Consultation on the Evaluation of the GDPR (28 de abril de 2020)
Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?	A LGPD exige que os controladores e operadores mantenham registros das atividades de tratamento de dados (Artigo 37) e não fornece detalhes sobre o que tais registros devem conter. A manutenção de tais registros pode ser onerosa dependendo do nível de tratamento de dados da organização, em particular para as PMEs que têm recursos limitados. Entretanto, é importante que as organizações compreendam o ciclo de vida dos dados e suas atividades de tratamento, pois isso (i) servirá de base para sua abordagem baseada em risco, accountability e esforços de conformidade com a LGPD, e (ii) lhes permitirá inovar e identificar novas oportunidades de negócios envolvendo o uso responsável dos dados. Portanto, a ANPD não deve isentar as PMEs de manter registros de atividades de tratamento. Pelo contrário, **a ANPD deve aplicar uma interpretação flexível e ampla às exigências da LGPD no que diz respeito aos registros de atividades de tratamento de dados, evitando com que essas regras sejam muito prescritivas, com foco em resultados desde que organizações compreendam quais dados elas coletam, o ciclo de vida dos dados e suas atividades de tratamento**. A ANPD poderia fornecer modelos às PMEs de maneiras simplificadas para manter registros das atividades de tratamento de dados, divulgar ferramentas disponíveis no mercado e explicar como PMEs podem conduzir o registro das atividades de tratamento de forma simultânia a

	outras atividades relacionadas para fins de eficiência (por exemplo, definir as bases legais para tratamento de dados e realizar avaliações de risco).
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	O artigo 31, §3º da LGPD prevê que a ANPD pode estabelecer regras complementares em relação à definição e às competências do encarregado, incluindo casos de isenção de acordo com a natureza e o tamanho da organização, bem como com o volume das operações de tratamento de dados. Do ponto de vista de uma PME, esta possibilidade de isenção da ANPD é bem-vinda. Na maioria dos casos, as PMEs têm recursos limitados e pode ser muito oneroso exigir que elas nomeiem um encarregado (especialmente à luz da ausência de regras por parte da ANPD sobre a função do encarregado, o que levanta questões como, por exemplo, se o encarregado deve ser uma função dedicada em período integral ou se pode ser uma função temporária). Entretanto, **o CIPL recomenda que a ANPD aplique uma abordagem baseada em risco para permitir isenções relativas à nomeação de encarregados por PMEs**, bem como por startups, ONGs e universidades que podem ter extensas operações de tratamento de dadose mas recursos limitados. Por exemplo, a ANPD poderia estabelecer que as PMEs com atividades de tratamento de baixo risco nomeiem um ponto de contato para tais atividades, e as PMEs com atividades de tratamento de alto risco designem um encarregado (por exemplo, se a organização conduzir o tratamento de dados pessoais sensíveis ou dados de crianças, tratamento de dados em larga escala, atividades de tratamento complexas ou estruturas complexas envolvendo o tratamento de dados). A obrigação de nomear um encarregado deve ser avaliada no caso a caso pela organização com base em um conjunto de critérios exemplares, como o risco de operações de tratamento, se os dados sensíveis são ou não tratados, o volume de tratamento de dados, etc. No entanto, **a ANPD deve esclarecer em suas orientações que todas as organizações, incluindo as PMEs, devem atribuir a responsabilidade por suas atividades de cumprimento da LGPD e seu programa de governança de dados a um indivíduo apropriado dentro da organização, mesmo que ele trabalhe em uma função diferente e não cumpra formalmente a função de encarregado**. Além disso, como mencionamos mais adiante nesta resposta do CIPL, a ANPD deve fornecer diretrizes e exemplos concretos para apoiar as PMEs e outras organizações a realizarem avaliações de risco. A orientação da ANPD também deve ser baseada em resultados, ou seja, **incentivar uma interpretação flexível dos requisitos relacionados ao encarregado para permitir que as PMEs alcancem os melhores resultados possíveis protegendo dados pessoais em seu contexto e circunstâncias específicos**, incluindo seu tamanho, tipo de organização, tipo de atividades de tratamento de dados e recursos ou falta de recursos. Em

	particular, a orientação da ANPD deve cobrir os seguintes tópicos que são fundamentais para permitir flexibilidade às PMEs no que diz respeito à nomeação de um encarregado: • **Encarregados em período integral versus encarregados temporários** – diferentemente da GDPR, a LGPD não tem requisitos específicos relativos à independência dos encarregados e aos conflitos de interesse, o que permite flexibilidade no que diz respeito à nomeação de encarregados que também desempenham outras funções no âmbito das organizações. Para muitas PMEs, ter um encarregado de forma temporária seria mais adequado do que um encarregado em período integral, pois muitas vezes há apenas uma pessoa responsável pela área de direito e compliance; e • **Encarreados internos versus encarregados externos/"encarregado como serviço"** – geralmente, o encarregado externo pode ser particularmente apropriado para as PMEs (embora possa ser muito caro para a maioria), pois garantiria que elas tivessem o nível necessário de conhecimento e experiência em proteção de dados dentro de suas organizações sem incorrer em encargos administrativos e financeiros substanciais (por exemplo, as PMEs e as startups teriam que remunerar o encarregado externo apenas por suas horas de trabalho). Entretanto, em alguns casos, os encarregados internos podem ser mais apropriados até mesmo para as PMEs, por exemplo, quando elas são ágeis e têm um modelo de negócios primordialmente baseado no tratamento de dados, o que pode sugerir que elas precisam de uma pessoa no local que esteja lá quase todos os dias, que esteja integrada aos negócios e, portanto, tenha um bom entendimento de como a empresa funciona e dos tratamentos de dados relacionados. Por exemplo, as PMEs e, em particular, as startups podem precisar de alguém que trabalhe mais intensamente com elas no início de seu estabelecimento como uma empresa para ajudá-las a estabelecer seus serviços, e depois ter alguém mais em meio período para garantir que a privacidade dos dados seja tratada de forma contínua. Portanto, é importante que a ANPD proporcione flexibilidade às PMEs em relação à nomeação do papel do encarregado e esclareça as circunstâncias em que as PMEs ficarão isentas das obrigações formais de nomeação. Mesmo se isentas, algumas PMEs podem decidir nomear um encarregado por razões estratégicas e comerciais (por exemplo, aumentar a confiança do consumidor/cliente, aumentar os poderes de concorrência). As PMEs que são operadoras também podem querer nomear um encarregado pelas mesmas razões. A nomeação de um encarregado deve ser vista como boa prática e uma forma de as organizações demonstrarem accountability, uma vez que a governança dos dados é uma das principais ferramentas que organizações têm de fazerem usos responsáveis de dados pessoais. Portanto, **a ANPD deve incentivar a**

	nomeação do encarregado ou de uma pessoa com responsabilidades equivalentes para todas as organizações, incluindo as PMEs, mesmo quando estas estão isentas de tal nomeação ou caracterizadas como operadoras. Finalmente, **a ANPD também deve incentivar a criação de uma rede/comunidade de encarregados** no Brasil. Isto poderia ser específico para setores, tamanho, regiões no Brasil. Essa rede/comunidade seria particularmente relevante para as PMEs, pois permitiria o compartilhamento de informações, boas práticas e *benchmarking*, o que facilitaria o treinamento dos encarregados e, em última instância, melhoraria o cumprimento da LGPD entre as PMEs. Veja como referência os seguintes documentos do CIPL sobre a função do encarregado sob a GDPR: • Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation (17 de novembro de 2016) • The Role of the Data Protection Officer (DPO) and Risk and High Risk under the GDPR (5 de outubro de 2016)
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Os relatórios de impacto são um dos mecanismos que as organizações podem utilizar para avaliar os riscos relacionados às suas atividades de tratamento de dados, que são fatores determinantes de accountability (veja nossa resposta à pergunta: "Quais são os impactos para as PMEs de estabelecer uma avaliação sistemática dos riscos à privacidade e à proteção de dados?"). A LGPD não exige explicitamente que as organizações realizem relatórios de impacto, exceto quando a ANPD o exigir (Artigo 10, parágrafo 3 e Artigo 38). Além disso, a LGPD não fornece muitos detalhes sobre o que os relatórios de impacto devem conter, exceto que eles devem descrever os dados pessoais processados, a metodologia usada para coleta e garantia da segurança dos dados, bem como para a análise de risco, e quaisquer salvaguardas e medidas de mitigação de risco. **A ANPD deve buscar um equilíbrio entre fornecer orientações e modelos para as PMEs no que diz respeito às avaliações de risco (incluindo relatórios de impacto), manter a flexibilidade da LGPD sobre este tópico e vitar regras excessivamente prescritivas**. A ANPD deve incentivar as PMEs a realizar avaliações de risco, incluindo relatórios de impacto, da maneira e circunstâncias mais apropriadas à sua organização, desde que alcancem o resultado desejado da análise dos riscos para indivíduos e adoção de medidas de mitigação de tais riscos. Portanto, podem haver casos em que as PMEs sejam dispensadas de realizar relatórios de impacto formais desde que analisem o risco de outras maneiras. A escolha do processo ou metodologia aplicado para avaliações de risco e relatórios de impacto deve ser feita pelas organizações. Qualquer orientação da ANPD sobre o processo ou metodologia de avaliação de risco deve, portanto, ser baseada em princípios, abrangente e flexível. A ANPD pode fornecer modelos de relatórios de impacto para PMEs e outras organizações caso exija que elas realizem este tipo particular de avaliação

	de risco, mas deve deixar claro que tais modelos são voluntários e que as organizações podem usar outros modelos e metodologias apropriadas ao seu contexto, desde que cumpram os requisitos do artigo 38 da LGPD. A ANPD também deve fornecer exemplos para as PMEs de casos em que será exigido que elas elaborem um relatório de impacto. Veja o seguinte documento do CIPL sobre riscos e DPIAs: • Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (21 de dezembro de 2016)
Quais são os impactos da implementação do tratamento de dados, inclusive sensíveis e de crianças e de adolescentes, em conformidade com a LGPD aos agentes de pequeno porte?	As regras da LGPD relativas ao tratamento de dados aplicam-se igualmente aos controladores e operadores, independentemente de seu tamanho. A LGPD tem regras específicas relativas ao tratamento de dados sensíveis e dados relativos a crianças e adolescentes (artigos 11 a 14 da LGPD), que as PMEs também devem observar. Além disso, a ANPD deve exigir que as PMEs apliquem uma abordagem baseada em risco a suas atividades de tratamento de dados, o que incluirá a possível aplicação de medidas técnicas e organizacionais mais robustas ao tratamento desses tipos de dados, uma vez que eles provavelmente representarão um nível de risco mais elevado para os indivíduos envolvidos.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Conforme delineado em nossa resposta à pergunta, "Quais são suas sugestões para resolver estes problemas?" acima, os programas de governança de dados são escalonáveis e, portanto, podem ser implementados por PMEs, que deverão calibrar os elementos do programa de acordo com seu contexto, riscos e objetivos. A implementação de programas de governança de dados gera uma série de benefícios para as PMEs e, de modo mais geral, para a economia brasileira: • **As PMEs tornam-se mais atraentes como fornecedoras/operadoras para as organizações controladoras**, incluindo organizações maiores e internacionais – a implementação de programas de governança de dados é uma indicação de responsabilização, o que impulsiona as oportunidades de negócios ao assegurar a elegibilidade para parcerias comerciais que envolvem dados pessoais. As organizações envolvidas em atividades de tratamento de dados que dependem de fornecedores/operadores também precisam garantir que os dados pessoais sejam protegidos quando transferidos para tais fornecedores/operadores. Elas o fazem avaliando os riscos dos fornecedores e implementando cláusulas contratuais apropriadas. Os riscos relacionados à proteção de dados provavelmente serão menores, e a negociação de cláusulas contratuais de proteção de dados exigirá menos esforços, se os fornecedores tiverem medidas de proteção apropriadas em vigor, incluindo um programa de governança de dados;

	• **As PMEs podem usar seu programa de governança de dados como um diferencial competitivo** – elas podem ter uma vantagem competitiva sobre outras PMEs, uma vez que não apenas se tornam mais atraentes como fornecedoras/operadoras (ver ponto acima), mas também podem decidir usar seu programa de governança de dados como parte de sua estratégia de marca (por exemplo, dizendo que possuem mecanismos robustos para proteger os dados pessoais dos indivíduos). Se forem PMEs voltadas para o consumidor, elas podem usar isso também para aumentar a confiança do consumidor; • **O risco das PMEs de não conformidade com a LGPD e possíveis sanções da ANPD diminuirão** à medida que os programas de governança de dados equipem as PMEs com políticas, processos e mecanismos para cumprir com as diversas regras da LGPD. Isto evitará ações repressivas ou, no caso de execução da LGPD, possivelmente simplificará e reduzirá o impacto financeiro de tal execução, uma vez que a PME estaria equipada para demonstrar os seus esforços de conformidade à ANPD; • **Incentivar organizações de todos os tamanhos a implementar programas de governança de dados acabará por aumentar a confiança no ecossistema de dados brasileiro e possibilitará a inovação impulsionada pelos dados** – isto promoverá a economia digital brasileira e evitará que indivíduos se abstenham de usar serviços on-line por medo, por exemplo, de que seus dados pessoais estejam sujeitos a vazamentos. Isto ajudará a aumentar a confiança com outras partes interessadas, como a mídia, investidores, a ANPD, clientes e funcionários; • **Incentivar organizações de todos os tamanhos a implementar programas de governança de dados também possibilitará inovação derivada do uso de dados** – o aumento da conformidade com as regras da LGPD significa que as PMEs poderão extrair valor dos dados pessoais ao os utilizam de forma responsável, com accountability e em conformidade, o que lhes permitirá inovar através do tratamento de dados; e • **Encorajar organizações de todos os tamanhos a implementar programas de governança de dados também provavelmente diminuirá o número de violações de dados notificados à ANPD** – um elemento-chave dos programas de governança de dados é a implementação de avaliações sistemáticas de risco. Elas permitem às organizações detectar e mitigar as violações de dados de forma mais eficaz e eficiente. É provável que a ANPD receba menos notificações de vazamentos de dados que “podem resultar em riscos ou danos relevantes aos titulares dos dados” (Artigo 48, LGPD), pois as organizações estarão mais bem equipadas para evitar que tais riscos e danos ocorram.

Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	A ANPD não deve conceder isenções às PMEs em relação ao estabelecimento e implementação de políticas de segurança de dados e processos relacionados. Isto é particularmente importante porque a crise da COVID-19 desencadeou uma aceleração das interações e atividades digitais, inclusive entre todas as organizações, incluindo as PMEs, o que as deixa mais vulneráveis a ataques cibernéticos, bem como a violações de dados. A implementação de medidas de segurança de dados é, logo, importante não apenas para proteger os indivíduos, mas também para proteger os ativos e os negócios das PMEs. Ao contrário, **a ANPD deveria exigir que as PMEs implementem políticas, processos e ferramentas (medidas) de segurança de dados de acordo com o nível de risco de suas atividades de tratamento de dados para os indivíduos e a sociedade**. Estas medidas devem ser flexíveis, adaptáveis e preparadas para o futuro e não devem estar presas aos avanços atuais em matéria de segurança de dados. A ANPD deve trabalhar com o setor para identificar e fornecer às PMEs exemplos de diferentes tipos de medidas de segurança de dados (incluindo anonimização e pseudonimização), bem como estudos de caso demonstrando como tais medidas podem ser aplicadas para mitigar diferentes tipos de riscos e danos. Ela também deve ser orientada pelas normas internacionais de segurança de dados existentes, tais como as normas da indústria de cartões de pagamento (PCI) e as diferentes normas de segurança de dados ISO (veja aqui e aqui), pois estas já são comumente usadas globalmente e serão reconhecidas por organizações maiores com as quais as PMEs brasileiras trabalham como fornecedoras ou parceiras comerciais.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	A avaliação de riscos é um dos elementos essenciais da accountability e a **ANPD deve incluí-la como um elemento-chave em suas próximas regras e orientações relativas às PMEs**. A avaliação de risco significa equilibrar os interesses da organização e da sociedade contra os possíveis danos aos indivíduos e mitigar riscos da maneira mais adequada ao contexto do tratamento de dados. As avaliações de risco incluem o gerenciamento de riscos relacionados à privacidade em vários contextos, incluindo: (i) no programa de governança de dados, (ii) nas atividades de tratamento, produtos, serviços, tecnologias e aplicações, (iii) no uso de fornecedores e terceiros, (iv) em avaliações de risco contextuais, tais como avaliações de interesses legítimos e relatórios de impacto, (v) ao calibrar e revisar periodicamente esses vários tipos de avaliações de risco à luz de mudanças nos modelos de negócios, nas leis, na tecnologia e outros fatores internos e externos. É fundamental que as PMEs possam realizar avaliações de risco, pois estas lhes permitirão (i) tomar decisões informadas, (ii) priorizar suas atividades e recursos, e (iii) aplicar mecanismos de proteção de privacidade adequados ao contexto e baseados em risco, independentemente da tecnologia ou prática específica que está sendo avaliada.

Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	A portabilidade de dados é um mecanismo essencial para a economia digital. Ela permite que as pessoas transfiram prontamente seus dados pessoais de um serviço para outro em vez de ficarem "bloqueadas" em um determinado prestador de serviços. Este direito pode funcionar como um facilitador da confiança digital, da concorrência e do crescimento econômico, particularmente para as PMEs. **A ANPD deve trabalhar com várias partes interessadas, incluindo setores industriais e outros reguladores brasileiros, para compreender e maximizar os benefícios e oportunidades da portabilidade de dados para indivíduos e organizações, incluindo PMEs**. A regulamentação da ANPD sobre portabilidade de dados tem o potencial de impulsionar a padronização das regras de interoperabilidade relacionadas aos dados pessoais. Isto resultará em ganhos de eficiência para a economia digital brasileira, melhores e diversificados serviços para os consumidores, e o cumprimento deste direito de proteção de dados. Além de fornecer mais regras para as PMEs, a ANPD deve emitir regulamentos específicos sobre como implementar o direito à portabilidade de dados (Artigo 18, V da LGPD). Ao elaborar tais regulamentos, a ANPD deve trabalhar com a indústria para compreender seus desafios e necessidades em relação ao desenvolvimento de normas e formatos interoperáveis e os custos envolvidos na sua implementação, segurança da transmissão de dados, qualidade dos dados, tipos de dados a serem portados, bem como questões de concorrência e propriedade intelectual.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação nos agentes de pequeno porte?	Há uma série de mecanismos regulatórios que a ANPD poderia utilizar para promover a inovação pelas PMEs: • **Criação de sandboxes** – dada a notável transformação social e econômica ocasionada pela quarta revolução industrial, é fundamental que o Brasil permita a inovação derivada do tratamento de dados e, ao mesmo tempo, garanta o uso responsável dos dados e a proteção dos direitos e interesses dos indivíduos. As sandboxes representam um espaço seguro onde as PMEs podem inovar através do uso responsável de dados pessoais sob a supervisão e aconselhamento da ANPD. A ANPD deve considerar as várias possibilidades para a criação de sandboxes: (i) sanboxes que foquem em desafios específicos relacionados à proteção de dados (por exemplo, inteligência artificial), (ii) concentrada em um setor de indústria específico (por exemplo, setor *fintech*), e (iii) organizadas de forma trans-setorial em parceria com outras autoridades reguladoras, na medida em que os desafios de proteção de dados sejam comuns a várias áreas regulamentadas (por exemplo, consumidor, concorrência, setor financeiro, telecomunicações); • **Promoção do desenvolvimento de códigos de conduta, certificações, selos e marcas** – pois eles são instrumentos promissores para a proteção de dados e para permitir que organizações enfrentem questões difíceis e desafios

	específicos da indústria, demonstrem accountability e compartilhem boas práticas, o que é particularmente relevante para as PMEs; • **Possibilitando o compartilhamento de dados** – a importância do compartilhamento de dados pessoais entre governo e organizações se tornou mais proeminente no contexto da pandemia COVID-19, com inúmeros exemplos de instituições de pesquisa e universidades (as quais normalmente caracterizadas como PMEs) buscando acesso a dados pessoais para realizar análises relevantes e buscar soluções à pandemia. O acesso aos dados e a possibilidade de usá-los é uma necessidade para a inovação, e é particularmente relevante para as PMEs, pois elas naturalmente têm acesso a menos dados pessoais em comparação a organizações maiores, mais competitivas e tecnologicamente avançadas. A ANPD deve facilitar e promover o compartilhamento de dados no contexto da LGPD, estabelecendo regras e fornecendo diretrizes sobre o compartilhamento de dados conforme o seu Artigo 11, parágrafo 3 e Artigo 30. Veja como referência os seguintes documentos do CIPL: • Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice (8 de março de 2019) • CIPL Response to the EDPB's Guidelines on Codes of Conduct and Monitoring Bodies under the GDPR (29 de março de 2019)
SUGESTÕES DE DISPOSIÇÕES	
O CIPL não tem sugestões específicas de disposições.	