2021 | MARÇO

CONTRIBUIÇÃO À ANPD

TOMADA DE SUBSÍDIOS Nº 1/2021 DA ANPD

PMES, STARTUPS, EMPRESAS DE INOVAÇÃO E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS COM FINS ECONÔMICOS

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Cynthia Picolo

Gustavo Henrique Luz Silva

Isabela Maria Rosal Santos

Revisão:

Amanda Espiñeira

José Renato Laranjeira de Pereira

Imagem de Capa:

Witthaya Prasongsin, Getty Images Pro

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

ANPD Autoridade Nacional de Proteção de Dados

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

NOME DA INSTITUIÇÃO: Laboratório de Políticas Públicas e Internet - LAPIN[1]

CNPJ: 36.965.428/0001-16

O Laboratório de Políticas Públicas e Internet (LAPIN) é um think tank de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade. Para maiores informações sobre nossa atuação, visite nosso site: <https://lapin.org.br/>.

[1] Essa contribuição foi desenvolvida pelos seguintes membros do LAPIN: Amanda Espiñeira (e-mail: amanda@lapin.org.br), Cynthia Picolo (cynthia.picolo@lapin.org.br), Gustavo Henrique Luz Silva (e-mail: gustavo.luz@lapin.org.br), Isabela Maria Rosal Santos (e-mail: isabela@lapin.org.br) e José Renato Laranjeira de Pereira (e-mail: joserenato@lapin.org.br).

LAPIN
LABORATÓRIO DE POLÍTICAS PUBLICAS E INTERNET

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídios deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO - LAPIN**
Quais são os desafios/problemas regulatórios relacionados ao tema?	São vários os desafios relacionados à regulação do tratamento diferenciado e simplificado para microempresa, empresas de pequeno porte e startups ou empresas de inovação. O primeiro ponto, que está presente em toda a sistemática de proteção de dados pessoais, é a necessidade de encontrar um sistema regulatório que não impeça ou retarde o desenvolvimento das atividades de uma organização, em destaque as que envolvem grande fluxo de dados e o investimento em pesquisa e desenvolvimento. Para tanto, ainda é necessário encontrar e desenvolver formas regulatórias úteis para esse objetivo - seja através de edição de normas complementares ou pelas decisões administrativas da ANPD ou por formas de autorregulação, como guias de boas práticas ou códigos de conduta. A incorporação de toda essa estrutura regulatória heterogênea, composta por formas de autorregulação e de

	heterorregulação[2], também se põe como um desafio aos agentes desse ecossistema. Esse processo depende de larga conscientização dos agentes que estarão submetidos a essas formas regulatórias, algo que ainda é incipiente no Brasil (pesquisa do Serasa Experian revela que aproximadamente 50% das microempresas declaram ter pouco ou nenhum conhecimento sobre o novo cenário regulatório[3]). Além disso, há falta de disponibilidade de recursos humanos qualificados para trabalhar com os agentes de tratamento diferenciados e, ainda, deve-se considerar o valor da mão-de-obra desses profissionais. Então, a determinação de obrigações para os agentes de tratamento com regras diferenciadas também deve considerar a reduzida disponibilidade de recursos humanos em empresas de menor porte (ver item sobre política de segurança). Sobre esse tópico, destaca-se que é necessário

[2] A heterorregulação diz respeito a regras impostas por agentes que não fazem parte direta do mercado tratado, o que é de suma importância para a arquitetura de proteção de dados, onde o titular se encontra em situação de hipossuficiência. Destaca-se o papel da ANPD nesse processo, que ajudará no empoderamento do titular. Nesse sentido: "a heterorregulação do mercado de dados pessoais precisa levar em consideração outras fontes de regulação, tais como a autorregulação, a tecnologia e as soluções de mercado. Para isso, embora deva existir uma influência recíproca entre todos esses fatores, a relação entre eles deve ser intermediada e conformada pela heterorregulação, a quem cabe preservar os direitos básicos dos titulares de dados, inclusive por meio da delimitação do alcance dos demais meios de regulação. Se assim não for, é grande o risco de que as soluções de mercados sejam aquelas impostas unilateralmente pelos agentes econômicos mais poderosos e que acabem dominando todos os outros meios de integração social, inclusive o direito (...) Logo, o advento da LGPD envolve a superação de abordagens simplistas ou excessivamente ingênuas, no sentido de que a lei resolveria todos os problemas. Diante dos riscos envolvidos, é necessária reflexão profunda sobre como a lei deve dialogar com as demais formas de integração social e que cuidados devem ser tomados para que suas previsões não sejam descumpridas ou neutralizadas". FRAZÃO, A. **Objetivos e alcances da Lei Geral de Proteção de Dados.** In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. pp. 125 -126.

[3] SERASA EXPERIAN. **Como as empresas se preparam para atender à nova regulamentação.** 2020. Disponível em: <https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf>. Acesso em 01 mar. 2021.

	desenvolver a regulação sobre a nomeação do encarregado, inclusive considerando se haverá tratamento diferenciado para as PMEs e startups sobre a obrigatoriedade de indicação (ver tópico específico sobre o tema). Outro desafio a ser considerado é como estabelecer parâmetros para a classificação das empresas em alguma das categorias apresentadas (microempresas, empresas de pequeno porte, startups ou empresas de inovação), bem como traçar mecanismos para a equiparação dessa classificação com a de outras legislações internacionais. Por exemplo, em relação às microempresas e empresas de pequeno porte, o Brasil adota o critério de faturamento e número de funcionários para o enquadramento de uma empresa em determinado porte[4], enquanto outras legislações (p. ex.: Argentina[5]) consideram outros critérios para tal classificação, como a atividade desenvolvida pela empresa. Então, constitui um problema identificar qual a melhor forma de uma empresa de pequeno porte ter direito ao tratamento

[4] A União Europeia também adota esse modelo, conforme o Regulamento nº 651/2014.
A Decisão nº 702 da *Comunidad Andina de Naciones* (CAN) também utilizou o critério híbrido para classificação de Pequenas e Médias empresas. Disponível em: <https://www.ecolex.org/details/legislation/decision-no-702-sistema-andino-de-estadistica-de-la-pyme-lex-faoc115929/#:~:text=La%20presente%20Decisi%C3%B3n%20de%20la,materia%20de%20PYME%20que%20se>. Acesso em 19 fev. 2021.
[5] A classificação argentina leva em consideração o número de funcionários, o faturamento, mas também o tipo de atividade desempenhada pela empresa.
UCEMA. **Gobierno corporativo em micro, pequenas y medianas empresas de Argentina**. Buenos Aires, Argentina, 2020. Disponível em: <https://ucema.edu.ar/publicaciones/doc_trabajo.php>. Acesso em 20 fev. 2021.

	diferenciado sobre a matéria de proteção de dados - o critério adotado pelo Brasil pode ser insuficiente, talvez seja necessário considerar o tipo de atividade desempenhada pela empresa. No âmbito tributário brasileiro, por exemplo, também existe um tratamento diferenciado para empresas de diferentes portes, expresso pelos critérios para enquadramento no Simples Nacional, o que inclusive influencia na escolha da forma organizacional de uma empresa. Com isso, a criação de um tratamento diferenciado para questões de proteção de dados também afetará essa escolha de modelo, o que pode funcionar como incentivo para a criação de novas empresas. Por isso, uma possível solução seria a unificação dos agentes que recebem tratamento diferenciado, assim, o sistema de proteção de dados poderia se utilizar da arquitetura do Simples Nacional para o enquadramento no sistema diferenciado para micro e pequenas empresas. Contudo, o tratamento diferenciado não pode ser genérico, simplesmente trazendo regras sobre isenções para as micro e pequenas empresas ou empresas de inovação sem explorar as peculiaridades de cada uma dessas, porque a regulação também não deve incentivar, de alguma forma, a simulação de formas empresariais ou o aumento da informalidade.

	Ainda sobre o tema de modelo empresarial, também se mostra necessário desenvolver como ocorrerá o processo de autodeclaração de uma empresa como *startup*[6] ou como empresa de inovação. O acompanhamento e avaliação dessas declarações deverá considerar outras normativas sobre o tema. Deve-se ponderar se é necessário trazer uma definição rígida e *ex ante* do que seriam *startups* ou empresas de inovação ou se adotar-se-á um modelo de autodeclaração com avaliação *a posteriori* da ANPD. Outro desafio inerente à regulação da proteção de dados, é a adoção do modelo de avaliação de risco já utilizado em outros pontos da LGPD. Essas avaliações de risco geram diversas obrigações relacionadas à cooperação com a ANPD - como deveres de documentação (p. ex.: relatório de impacto à proteção de dados pessoais, relatório de legítimo interesse etc.), de término de tratamento e de respostas a requisições - a fim de garantir que os direitos dos titulares sejam observados e a privacidade preservada ao máximo. Contudo, é necessário dosar a quantidade de obrigações, já que mais obrigações poderiam impossibilitar o engajamento das empresas no processo de adequação às regras de privacidade.

[6] O "Marco Legal das *Startups*", fruto da consolidação do PLP 146/2019 e PLP 249/2020, teve seu texto aprovado pelo Senado em 24 de fevereiro de 2021. Esse documento define que "são enquadradas como *startups* as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados".

	Por fim, a ANPD deverá encontrar formas para garantir a conscientização e o engajamento dos agentes de tratamento com regime diferenciado, porque é crucial o desenvolvimento de uma cultura de proteção de dados para que a regulação proposta seja efetiva.
Existem sugestões para endereçamento do problema?	Apesar de a LGPD trazer em seu art. 55-J, XVIII, a necessidade de edição de "normas, orientações e procedimentos, simplificados e diferenciados" para microempresas e empresas de pequeno porte e startups e empresas de inovação, é necessário que tais resoluções sejam direcionadas especificamente para cada uma dessas formas empresariais, não de uma forma genérica, mas considerando quais tratamentos diferenciados se aplicam para cada uma delas. A ANPD deve desenvolver formas de acesso facilitado para cada manual específico, criando guias práticos de adequação. Tal material pode estar disponível no próprio site da ANPD, o que facilita a comunicação da autoridade com os agentes de tratamento, principalmente ao se considerar a dimensão continental do país. Iniciativa semelhante foi desenvolvida pela autoridade britânica Information Commissioner's Office - ICO, que reserva página específica de seu sítio eletrônico para orientações para empresas de pequeno porte[7]. Dentro desse endereço, existem guias práticos para a criação de avisos de privacidade, verificação do nível de adequação e outras indicações a fim de garantir maior segurança da

[7] Disponível em: <https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/>. Acesso em 20 fev. 2021.

	informação. Também apresentam direcionamentos em seus sites a IAPP[8], a Autoridade Australiana[9] a Autoridade Canadense[10], entre outras. Além disso, seria extremamente positivo se a ANPD oferecesse programas de conscientização e educação para pequenos empreendedores. Sugere-se também para isso o modelo eletrônico, para incentivar a propagação da cultura de privacidade por todo o Brasil e não só nos polos industriais, como Rio de Janeiro e São Paulo. Iniciativas como a plataforma de educação em LGPD[11] , desenvolvida pelo governo federal, são de extrema importância para atingir esse fim. A conscientização sobre as exigências regulatórias sobre o tema também deve alcançar investidores, de forma que os gastos com questões de privacidade não impeçam o desenvolvimento e o investimento em novas companhias, em especial *startups.* Ainda é necessário considerar o caráter global de diferentes empresas, principalmente as que trabalham diretamente com inovação, para o endereçamento das questões regulatórias (p. ex.:

[8] Associação Internacional dos Profissionais de Privacidade - Disponível em: <https://iapp.org/resources/article/sample-data-protection-policy-template-2/>.
[9] Officer of the Australian Information Commissioner, disponível em: <https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/>. Acesso 20 fev. 2021.
[10] Disponível em: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/>. Acesso em 20 fev. 2021.
[11] Disponível em <https://serpro.gov.br/menu/noticias/noticias-2021/plataforma-lgpd>. Acesso em 23 fev. 2021.

	possibilidade de reconhecimento de certificações internacionais, possibilidade de indicação de encarregado em outro país, etc). É possível observar experiências internacionais para delimitar quais empresas podem ser isentas das obrigações de privacidade, parcial ou integralmente. Por exemplo, a lei australiana de privacidade não é aplicável à maior parte do setor privado, apresentando uma lista sobre quais empresas estão submetidas às suas obrigações[12]. Essa determinação deve ocorrer considerando a realidade brasileira e a fraca cultura de segurança de dados existente atualmente, como identificado nos recentes escândalos de vazamentos de dados. Outro endereçamento é a consideração dos diferentes modelos empresariais na metodologia de aplicação de sanções administrativas e a regulação dessa lacuna da LGPD. As penas devem sim ter um caráter de conscientização e desincentivo, mas não devem ser a razão para a morte de uma empresa. Para tanto, uma abordagem que leve em conta modelos regulatórios baseados em regulação responsiva, incluindo ferramentas como a pirâmide regulatória, são bem vindos para garantir um racional de sanções escaláveis de acordo com as falhas incorridas pelo ente regulado.

[12] WATTS, D.; CASANOVAS, P. **Privacy and Data Protection in Australia: a Critical overview (extended abstract).** Disponível em: <https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf>. Acesso em 22 fev. 2021.

	Por fim, é de suma importância que a ANPD e outros órgãos relacionados disponibilizem meios de comunicação diretos para PMEs e outros agentes de tratamento sanarem dúvidas referentes à aplicação da legislação em prazo razoável. Esse diálogo deve ser dinâmico, para evitar qualquer incidente entre a comunicação do agente e a resposta da autoridade.
Quais são as oportunidades relacionadas ao tema?	A regulamentação diferenciada para microempresas, empresas de pequeno porte e startups é um momento de aproveitar diversas oportunidades e realizar sinergias que revolvem o tema. Segundo dados de 2020 da Receita Federal, extraídos do Painel de Empresas do Sebrae (DataSebrae)[13], de 19.228.025 (100%) empresas existentes no país, 9.819.483 (~51,69%) são Microempreendedores Individuais (MEI), 6.586.497 (~34,25%) são Microempresas (ME) e 896.336 (~4,66%) são Empresas de Pequeno Porte (EPP), ou seja, 90,6% das empresas brasileiras são PMEs. Pelo profundo papel que as PMEs exercem na economia nacional, uma regulamentação diferenciada da LGPD para estes agentes é essencial para a promoção do desenvolvimento econômico de grande parte da economia brasileira, observando-se os direitos fundamentais dos titulares de dados. Destaca-se algumas oportunidades centrais, quais sejam:

[13] Fonte: Receita Federal do Brasil, dados atualizados em 11 de maio de 2020. SEBRAE. **DataSebrae: Painel de empresas**. Disponível em: < https://datasebrae.com.br/totaldeempresas/>. Acesso em 22 fev. 2021.

	● A diminuição da pesada carga regulatória existente aos pequenos negócios no Brasil (o corriqueiramente denominado 'Custo Brasil'); ● A simplificação, flexibilização e facilitação de procedimentos da LGPD (por exemplo, dispensa de encarregado, relatório de impacto à proteção de dados simplificado, desnecessidade do registro de tratamento de dados); e ● O incentivo à inovação, à concorrência e ao desenvolvimento econômico e tecnológico. Também é uma oportunidade ímpar para que esta Autoridade exerça forte atuação nas frentes de conscientização, educação e *advocacy*, por meio da execução de algumas medidas: ● Explicar e clarificar conceitos centrais da lei (bases legais, agentes de tratamento, direitos dos titulares, responsabilidade civil dos agentes de tratamento etc.); ● Elaborar guias operacionais, templates (modelos) diversos, checklists, ferramentas e páginas interativas para auxiliar na avaliação, implementação e na contínua conformidade da LGPD por parte das PMEs; ● Responder a consultas e aconselhamentos específicos, solicitados pelas PMEs por meios eletrônicos (e-mail, formulário, SEI etc.), por correspondência e por telefone; ● Definir e promover padrões técnicos de segurança da informação aplicáveis às PMEs; e

	● Realizar seminários, *webinars*, workshops e conferências para a difusão da LGPD nas PMEs. Nesse sentido, a ANPD tem uma grande oportunidade em mãos de capilarizar a difusão da disciplina de proteção de dados por todo o país, contribuindo para a esperada mudança de cultura de proteção de dados no Brasil, em linha com os objetivos estratégicos 1 e 2 dispostos no Planejamento Estratégico 2021-2023 desta Autoridade.
Quais são as experiências internacionais sobre o tema?	O Regulamento Europeu de Proteção de Dados ('GDPR' ou 'Regulamento'), a Lei de Privacidade do Consumidor da Califórnia ('CCPA') e a Lei de Privacidade Australiana preveem derrogações a micro, pequenas e médias empresas ('PME') e, portanto, merecem destaque dentre as experiências internacionais sobre o tema. Como tanto as boas práticas quanto as dificuldades enfrentadas no exterior contribuem para uma melhor compreensão sobre a aplicabilidade de um ato normativo e, porque o caráter transfronteiriço da economia digital permite que empresas de qualquer porte possam deter esse aspecto internacional, entendemos ser importante incluir em nossa contribuição alguns desafios citados pelas PMEs, principalmente as europeias. É interessante observar que muitos dos desafios citados pelas PMEs estrangeiras foram também apontados no relatório do Serasa Experian, que entrevistou empresas de todos os portes, incluindo PMEs, sobre os desafios da adequação à LGPD. Segundo as pesquisas, 25% das que declararam ter pouco ou

nenhum conhecimento da legislação são microempresas, e muitas ainda não sentem necessidade de iniciar os processos de adequação. Além disso, microempresas (23%) e empresas de pequeno porte (13%) confirmaram que, apesar da previsão, ainda não investiram em medidas de segurança de dados. O treinamento de funcionários, a falta de recursos financeiros e de pessoal qualificado também foram destacados como grandes desafios[14].

Estas e outras questões foram igualmente reportadas no cenário internacional, que a seguir analisamos:

(1) União Europeia - GDPR[15]

O conceito de "empresa" no GDPR é definido no artigo 4(18) como sendo uma pessoa física ou jurídica, independente de sua forma, que exerce atividade econômica, incluindo parcerias ou associações que exercem regularmente uma atividade econômica. Estas entidades estão sujeitas aos direitos e obrigações definidos no GDPR, porém, com alguma flexibilidade.

[14] Foram realizadas duas pesquisas: em 2019, com 508 empresas, e em 2020, com 513 empresas, sendo 238 microempresas e 74 de pequeno porte. Serasa Experian, **Relatório: Como as empresas se preparam para atender à nova regulamentação** (17/11/2020). Disponivel em: <www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf>. Acesso em 22 fev. 2021.

[15] **General Data Protection Regulation**. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 22 fev. 2021.

	O Considerando 13 do GDPR faz menção à derrogação prevista às PMEs e deixa claro que as instituições e órgãos da UE, bem como os Estados-Membros e respectivas autoridades de proteção de dados, são incentivados a levarem em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do Regulamento. Ainda, o Considerando aconselha a seguir a noção de micro, pequenas e médias empresas prevista no artigo 2º do Anexo da Recomendação da Comissão 2003/361/CE[16], que possui as seguintes definições: 1. *A categoria das micro, pequenas e médias empresas (PMEs) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros, e/ou cujo balanço total anual não excede 43 milhões de euros;* 2. *Na categoria das PMEs, uma pequena empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede 10 milhões de euros;* 3. *Na categoria das PMEs, uma microempresa é definida como uma empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.*

[16] Comissão Europeia, **Recomendação de 6 de maio de 2003 relativa à definição de micro, pequenas e médias empresas** (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36). Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/6ca8d655-126b-4a42-ada4-e9058fa45155/language-en>. Acesso em: 22 fev. 2021.

	Neste sentido, e dando efeito ao Considerando 13, o artigo 30(5) do GDPR prevê que empresas ou organizações com menos de 250 pessoas não precisam registrar as atividades de tratamento, a menos que (i) possam implicar um risco para os direitos e liberdades do titular dos dados; (ii) o tratamento não seja ocasional; (iii) o tratamento abranja dados pessoais sensíveis; ou (iv) relativos a condenações criminais e infrações. Em seu primeiro relatório de avaliação do GDPR, a Comissão Europeia ('CE') reforçou que de acordo com a abordagem baseada no risco ('risk-based approach') adotada no GDPR, não seria adequado prever derrogações com base na dimensão dos responsáveis pelo tratamento, já que os riscos para os titulares não dependem deste critério[17]. **- Desafios às PMEs**

[17] Comissão Europeia, **Communication from the Commission to the European Parliament and the Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation** (24/06/2020). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> p. 9. Acesso em: 22 fev. 2021.

	No âmbito do projeto BOOST, a Autoridade Belga de Proteção de Dados divulgou um relatório em agosto de 2020 sobre o conhecimento e compreensão do GDPR pelas PMEs[18]. Damos destaque às conclusões sobre os seguintes temas: ● **Conceitos de "controlador" e "operador"**: apenas pouco mais da metade das PMEs entrevistadas têm conhecimento satisfatório sobre tais conceitos, e a maioria admitiu que compreender o papel e as responsabilidades destes dois atores não é suficiente; ● **Princípio da transparência**: falta conhecimento teórico sobre as declarações de privacidade, embora a maioria delas indique conformidade com as obrigações do GDPR. Ainda, pouco mais da metade das empresas participantes não seguem um procedimento padrão para informar os titulares dos dados sobre as operações de tratamento de dados; ● **Relatório de impacto à proteção de dados pessoais ('DPIA')**: grande parte das PMEs têm pouco conhecimento sobre as situações em que o DPIA deve ser conduzido e como realizá-lo corretamente.

[18] Autorité de protection de données, **La Connaissance et la Comprehension du Reglement General sur la Protection des donnés (RGPD) Au sein des PME.** Disponível em: <www.autoriteprotectiondonnees.be/publications/rapport-sur-la-connaissance-et-la-comprehension-du-rgpd-au-sein-des-pme.pdf>. Acesso em 22 fev. 2021. Ver abaixo mais informações sobre o projeto BOOST.

	Neste mesmo relatório, as PMEs também mencionaram desafios abrangendo as seguintes questões: ● Período de retenção dos dados pessoais; ● Registro das operações de tratamento de dados; ● Subcontratação de terceiros; e ● Os princípios de proteção de dados *by design* e *by default*. Além disso, entidades europeias apontaram outras dificuldades enfrentadas pelos agentes de tratamento submetidos ao regime diferenciado: ● **Comitê Europeu de Proteção de Dados** (*European Data Protection Board* – 'EDPB') reconheceu que a implementação do GDPR tem gerado encargos administrativos às PMEs[19]; ● **A Comissão Europeia** apontou que PMEs e as startups relatam ter dificuldade para implementar o princípio da *accountability*, especialmente porque nem sempre recebem orientação e conselhos práticos suficientes das Autoridades de Proteção de Dados, ou porque o tempo necessário para obter aconselhamento é muito longo. Foram mencionados casos em que

[19] EDPB, **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf> p. 3. Acesso em: 22 fev. 2021.

	Autoridades exitaram em se envolver em questões legais. Diante de tais situações, as PMEs optam por recorrer a consultores e advogados externos para lidar com a implementação do princípio da *accountability*[20] e entender a abordagem baseada no risco (incluindo transparência, registro de operações de tratamento de dados pessoais e notificações de incidente de segurança), gerando, portanto, custos adicionais[21]; • **SMEUnited** (Associação Europeia de Artesanato e de Pequenas e Médias Empresas) citou **(i)** a falta de compreensão sobre quais medidas de segurança precisavam ser implementadas, especialmente nas microempresas[22]; **(ii)** a necessidade de modificação dos termos e condições para informar clientes sobre seus direitos em matéria de proteção de dados pessoais e sobre o responsável pelo tratamento gerou mais encargos administrativos[23]; **(iii)** o tempo gasto pelos controladores para educar os titulares dos dados sobre o escopo de seus direitos e, consequentemente, a extensão das respostas fornecidas[24]; **(iv)** a falta de recursos e de tempo, faz com que as micro e pequenas empresas ainda não considerem a proteção de dados pessoais

[20] Artigo 5(2) GDPR.
[21] Documento de Trabalho da Comissão Europeia, que acompanha o **Communication from the Commission to the European Parliament and the Council** (n. 3). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0115&from=EN> p. 24. Acesso em: 22 fev. 2021.
[22] SMEunited Crafts & SMEs in Europe, **Input to the Questions to Inform the Preparation of the Evaluation Reporto of May 2020 on the Application of GDPR** (Março 2020). Disponível em: <www.smeunited.eu/admin/storage/smeunited/contributions-members-gdpr-2020.pdf> p. 1. Acesso em 22 fev. 2021.
[23] Ibid, p. 3.
[24] Ibid, p. 6.

	uma prioridade[25]; **(v)** além do alto custo para implementar medidas, treinar e contratar novos funcionários, foi mencionada a dificuldade de encontrar encarregados ('DPOs') que tenham conhecimentos jurídicos e setoriais[26]; • **Conselho da União Europeia** relatou que de acordo com alguns Estados-Membros, PMEs não estão satisfeitas com a derrogação do artigo 30(5) do GDPR em relação à obrigação de manter um registro operações de tratamento de dados pessoais já que as condições são raramente aplicáveis[27]; • **BusinessEurope** (Confederação das Empresas Europeias) ressaltou que (i) PMEs muitas vezes têm adotado ações extremamente diligentes, mesmo quando não necessárias, para estarem em conformidade com empresas maiores, por medo de retaliação da Autoridade de Proteção de Dados competente, ou porque esclarecer dúvidas geralmente leva mais tempo que implementar a ação em si. O *approach* preventivo tem gerado encargos administrativos e processos onerosos que talvez sejam desproporcionais às intenções do GDPR[28]; (ii) as PMEs têm dificuldade em

[25] Ibid, p. 2.
[26] Ibid, p. 12.
[27] Conselho da União Europeia, **Council position and findings on the application of the General Data Protection Regulation** (19/12/2019). Disponível em: <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf> p. 13. Acesso em: 22 fev. 2021.
[28] BusinessEurope, **Position Paper: Review of the General Data Protection Regulation** (29/11/2019). Disponível em: <www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2019-11 29_be_gdpr_review.pdf> pp. 5-6. Acesso em: 22 fev. 2021.

definir a base legal adequada para o tratamento dos dados, levando-as a utilizarem o consentimento na maioria das vezes[29]; (iii) a restrição à aplicação da derrogação do artigo 30(5) do GDPR quando o tratamento de dados pessoais não é ocasional foi alvo de críticas.[30] Foi mencionado que o EDPB fez uma interpretação muito rigorosa ao entender que o tratamento regular de dados de funcionários não pode ser considerado ocasional[31]

(2) EUA, Califórnia - CCPA[32]

De acordo com a Lei de Privacidade do Consumidor da Califórnia, as obrigações contidas na legislação aplicam-se a empresas com fins lucrativos que fazem negócios na Califórnia e atendam a qualquer um dos seguintes critérios[33]:

- Empresas com receita bruta anual superior a $25 milhões;

[29] Ibid. p. 6.
[30] Id.
[31] Working Party 29, **Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR** (19/04/2018). Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045>. Acesso em: 22 fev. 2021.
[32] California Consumer Privacy Act. Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121>. Acesso em: 22 fev. 2021.
[33] ibid, SEC. 9. Section 1798.140 of the Civil Code. Ver também *State of California Department of Justice - Office of the General Attorney*. Disponível em <https://oag.ca.gov/privacy/ccpa>. Acesso em 22 fev. 2021.

	• Empresas que, sozinhas ou em combinação, anualmente compram, recebem, vendem ou compartilham para fins comerciais informações pessoais de 50.000 ou mais consumidores, famílias ou dispositivos; ou • Empresas que obtêm 50% ou mais de sua receita anual com a venda de informações pessoais de consumidores. Em uma pesquisa conduzida pela *International Association of Privacy Professionals* (IAPP)[34], foram destacados alguns desafios que a CCPA representa às PMEs, tais como • A exigência de clientes para que as empresas se adequem à CCPA, mesmo que a legislação não seja aplicável àqueles negócios; • Os profissionais de privacidade são frequentemente os mais experientes, porém dedicam apenas metade do tempo a temas relacionados à privacidade, priorizando as expectativas do cliente e a prevenção de ameaças e ataques ao invés da conformidade regulatória e legal;

[34] FENNESSY, Caitlin. **The unique challenges CCPA poses for SMEs** (05/09/2019). Disponível em: <https://iapp.org/news/a/the-unique-challenges-ccpa-poses-for-smes/>. Acesso em: 22 fev. 2021.

	• PMEs têm orçamentos menores e investem com menos frequência em treinamento de privacidade; • Falta de clareza na lei, principalmente (i) se dados de funcionários são cobertos; (ii) como a "venda" de dados se relaciona com a publicidade básica; e (iii) sobre como lidar com potenciais conflitos de lei; • Por não terem programas de privacidade tão robustas quanto grandes empresas, a gestão de fornecedores também pode representar um desafio; • A revisão das disposições contratuais relacionadas a processamento de dados exigirá tempo e recursos significativos, incluindo em assessoria jurídica externa. **(3) Privacy Act - Austrália** [35]

[35] Privacy Act 1988. Disponível em: <https://www.legislation.gov.au/Details/C2021C00024>. Acesso em: 22 fev. 2021.

	A Lei de Privacidade Australiana prevê uma série de isenções em relação a sua aplicação, incluindo a pequenas empresas com um faturamento anual de até $3 milhões[36]. No entanto, a lei cobre certos negócios independente do faturamento, como: ● Provedores de serviços de saúde; ● Negócios que comercializem informações pessoais; ● Contratantes que forneçam serviços sob um contrato da Commonwealth; ● Operadores de banco de dados de locação residencial; ● Órgãos de informações de crédito; ● Entidades que prestem informações para fins da Lei de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo; ● Associações de funcionários registradas ou reconhecidas pela Fair Work Act 2009; ● Empresas que conduzam votações secretas ('protected action ballot') no contexto da Fair Work Act 2009; ● Empresas credenciadas no sistema Consumer Data Right; ● Negócios relacionados a outros que sejam cobertos pela Lei de Privacidade;

[36] ibid, Divisão I, Subseção 6D. De acordo com a Parte II, Divisão I, Subseção 6DA da lei, isso inclui: (a) receita da venda de bens e/ou serviços; (b) receita de comissões; (c) receita de reparos e serviços; (d) renda de aluguel, arrendamento e locação; (e) recompensas e subsídios do governo; (f) juros, royalties e dividendos; (g) outras receitas operacionais.

	● Empresas prescritas pela Privacy Regulation 2013; ● Empresas que optaram por serem cobertas pela Lei de Privacidade[37]. A Autoridade de Proteção de Dados Australiana (OAIC) elaborou um *Privacy Checklist for Small Business*[38] para ajudar pequenas empresas a entenderem se estão sujeitas à Lei de Privacidade.
Quais são os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte?	Diante dos exemplos internacionais, cabe à ANPD levar em consideração os seguintes critérios quando da normatização da regulamentação de definição de agentes de tratamento de dados de pequeno porte: ● o faturamento da empresa; ● o porte/tamanho da empresa; ● o nº de funcionários da empresa;

[37] A Autoridade de Proteção de Dados Australiana – *Office of the Australian Information Commissioner* – compilou tais situações cobertas pela lei. Disponível em: <www.oaic.gov.au/privacy/privacy-for-organisations/small-business/>. Acesso em: 22 fev. 2021.

[38] OAIC, **Privacy Checklist For Small Business.** Disponível em: <www.oaic.gov.au/privacy/privacy-for-organisations/small-business/#PrivacyChecklistForSmallBusiness>. Acesso em: 22 fev. 2021.

	• se a empresa tem como modelo de negócios o tratamento de dados - os códigos de classe e subclasse do CNAE/IBGE[39] podem ser extremamente úteis para trazer aspectos mais objetivos a esse critério; e • volume de dados tratados e titulares atingidos pelos tratamentos de dados da empresa numa base periódica (p. ex., mensal, semestral, anual). Cabe salientar que, na Lei de Privacidade Australiana, há exceções às isenções da lei para PMEs quando estas empresas são de setores estratégicos e/ou que majoritariamente tratam dados pessoais e/ou sensíveis no âmbito do modelo de negócio, como provedores de serviços de saúde, negócios que comercializam informações pessoais, dentre outros. Exceções do tipo na regulamentação desta Autoridade também serão imprescindíveis para a manutenção de um campo regulatório justo e competitivo a todos os entes envolvidos.
Como a União Europeia tem atuado para que	Diversas ações voltadas especificamente às PMEs para ajudá-las a estarem em conformidade com o GDPR vêm sendo adotadas na União Europeia. As iniciativas partem não somente das Autoridades de

[39] É possível ter acesso a alguns códigos de classificação já disponíveis, inclusive relacionados a tratamento de dados. Disponível em: <https://cnae.ibge.gov.br/?option=com_cnae&view=atividades&Itemid=6160&tipo=cnae&chave=dados&versao_classe=7.0.0&versao_subclasse=>. Acesso em 01 mar. 2021.

agentes de tratamento de dados de pequeno porte estejam em conformidade com a *General Data Protection Regulation* (GDPR)?	Proteção de Dados, mas também da Comissão Europeia (CE), que financia projetos para esta finalidade.[40] Além disso, vale ressaltar que a CE se comprometeu a estudar propostas para possíveis alterações às disposições do GDPR no que diz respeito aos registros de tratamento de dados por PMEs que não possuem o processamento de dados pessoais como atividade principal, sendo, portanto, de baixo risco no que se refere à proteção de dados.[41] O EDPB também declarou estar empenhado em facilitar o desenvolvimento de ferramentas pelas Autoridades de Proteção de Dados para apoiar PMEs de modo a aliviar ao máximo seus encargos administrativos.[42] Este compromisso foi inclusive reforçado em seu Planejamento Estratégico de 2021-2023.[43]

[40] A descrição de alguns projetos está disponível em: <http://ec.europa.eu/research/participants/portal/doc/call/rec/rec-rdat-trai-ag-2017/1845149-project_abstracts_rec-rdat-trai-ag-2017_en.pdf>. Acesso em: 22 fev. 2021.

[41] Comissão Europeia, **Communication from the Commission to the European Parliament and the Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation** (24/06/2020). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> p. 15. Acesso em: 22 fev. 2021.

[42] EDPB, **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf>, p. 3. Acesso em: 22 fev. 2021.

[43] EDPB Strategy 2021-2023. Ver **Pilar 1: Avançando a Harmonização e Facilitando *Compliance* – Ações n. 1 e 3**. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf>, pp. 3-4. Acesso em: 22 fev. 2021.

	De maneira geral, as ações desenvolvidas pelas Autoridades de Proteção de Dados às PMEs incluem: ● Publicação de guias específicos, alguns interativos; ● Estabelecimento de linha direta de comunicação (*'hotline'*) para consulta e aconselhamento; ● Participação em seminários, workshops e conferências; ● Elaboração de modelos para registro de operações de tratamento de dados pessoais, avisos de privacidade e comunicação de incidente de segurança; ● Checklist para verificar *compliance* e orientações para condução do DPIA. A CE relembrou que o GDPR disponibiliza ferramentas importantes e que devem ser usadas para fins de *compliance*, como códigos de conduta, mecanismos de certificação e cláusula contratual padrão[44].

[44] EDPB, **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf>, p. 9. Acesso em: 22 fev. 2021.

<table>
<tr><td></td><td>Disponibilizamos, ao final deste documento, o Anexo I, composto por uma descrição detalhada das atividades realizadas pelas Autoridades Europeias de Proteção de Dados</td></tr>
<tr><td>Quais são os impactos para agentes de pequeno porte da manutenção do registro das operações de tratamento de dados pessoais?</td><td>O art. 37 da LGPD determina que “o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”. Ou seja, estes agentes devem elaborar uma espécie de inventário com diversas informações das operações realizadas, desde a coleta do dado até sua exclusão.

Como a LGPD não menciona os elementos necessários que devem constar neste registro, é interessante observar o que o GDPR dispõe sobre o tema, já que ela lista as informações que devem ser registradas e que são diferentes para controlador e operador:

<table>
<tr><th>Artigo 30 GDPR (controlador)</th><th>Artigo 31 GDPR (operador)</th></tr>
</table>
</td></tr>
</table>

	• O nome e contato do controlador e, quando aplicável, do controlador conjunto, do representante do controlador e do DPO; • A finalidade do tratamento; • A descrição das categorias dos titulares de dados e dos dados pessoais; • As categorias de destinatários a quem os dados foram ou serão divulgados, incluindo destinatários em países terceiros ou organizações internacionais; • Informações relativas à transferência internacional de dados pessoais, incluindo a organizações internacionais; • O prazo para exclusão das diferentes categorias de dados; • As medidas técnicas e organizacionais de segurança.	• O nome e contato do operador e contro e, quando aplicável, do representante controlador ou operador e do DPO; • As categorias de tratamento realizadas determinação do controlador; • Informações relativas à transferência internacional de dados pessoais, inclui organizações internacionais; • As medidas técnicas e organizacionais segurança.

	Para fins comparativos, no Brasil, o Governo Federal sugeriu registrar as seguintes informações no âmbito da Administração Pública:[45] ● Agentes de tratamento e o encarregado; ● Finalidade do tratamento; ● Base legal; ● Previsão legal; ● Dados pessoais tratados pela instituição; ● Categoria dos titulares dos dados pessoais; ● Tempo de retenção dos dados pessoais; ● Instituições com as quais os dados pessoais são compartilhados; ● Transferência internacional de dados;

[45] Governo Federal, **Guia de Elaboração de Inventário de Dados Pessoais** (20/09/2020). Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf>. Acesso em: 22 fev. 2021.

	● Medidas de segurança adotadas. Independentemente de quais informações deverão obrigatoriamente constar no registro das operações de tratamento de dados pessoais, este, por si só, certamente representa um grande desafio aos agentes de pequeno porte, especialmente levando em consideração que a LGPD traz uma definição bastante ampla do conceito de tratamento de dados, abrangendo mais de 20 ações.[46] Assim como registrar as operações de tratamento de dados pessoais exige, no mínimo, conhecimento jurídico, técnico e investimento financeiro, a manutenção do registro demandará os mesmos esforços, senão adicionais, especialmente considerando que se trata de um exercício contínuo[47] para os agentes de tratamento. Por outro lado, é importante destacar os aspectos positivos da manutenção do registro das operações de tratamento: além de trazer segurança jurídica aos atores envolvidos, ela atende a diversos requisitos estabelecidos pela LGPD, como, por exemplo, o cumprimento dos princípios da transparência, do livre acesso e da responsabilização e prestação de contas, e é também relevante para fins de

[46] Artigo 5º X LGPD. BIONI, Bruno R. **A obrigação de registro das atividades de tratamento de dados** (JOTA, 21/08/2019). Disponível em: <www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-obrigacao-de-registro-das-atividades-de-tratamento-de-dados-21082019>. Acesso em: 22 fev. 2021.
[47] *Ibid*.

	fiscalização pela ANPD. Porém, a realidade dos agentes de pequeno porte deve ser levada em consideração quando se trata dos impactos que a elaboração e manutenção deste registro terá sobre eles. As experiências internacionais mostram que, no geral, PMEs têm dificuldades para entender os requisitos da lei e a classificação das bases legais, e não sabem como registrar as atividades de tratamento, muitas delas recorrendo a consultorias externas ou deixando questões de privacidade e proteção de dados em segundo plano. Ademais, vale ressaltar que a manutenção do registro de tratamento de dados requer, pelo menos, uma estrutura organizacional robusta, com programas de governança, processos internos bem definidos, treinamentos constantes e políticas específicas. Todos esses fatores tendem a criar encargos financeiros e administrativos desproporcionais aos fundamentos da lei, particularmente no que se refere ao desenvolvimento econômico, tecnológico e à inovação.[48] Desta forma, considerando os casos em que a manutenção do registro de tratamento de dados deve ser obrigatória (alto risco), a realidade das PMEs exige procedimentos adequados de modo a não

[48] LGPD, artigo 2°, V.

	comprometer o funcionamento do negócio - relatórios simplificados, utilização de modelos de registro padrão, entre outros.
Quais são os impactos da nomeação de um encarregado de dados aos agentes de pequeno porte?	Com foco na presente tomada de subsídios, e independentemente da regulamentação específica sobre a figura do encarregado (art. 5º, VIII da LGPD), em relação ao formato que poderá ser configurado dentro das organizações (funcionário do agente de tratamento, equipe de funcionários, prestadores de serviço terceirizados, etc.) ou suas atribuições, é relevante a análise do impacto da obrigação estipulada no art. 41, caput, da LGPD, às pequenas empresas. O art. 41, § 3º da LGPD possibilita à ANPD a dispensa da necessidade de indicação do encarregado do tratamento de dados pessoais conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. Tendo em vista as obrigações mínimas do encarregado, nos termos do § 2º do art. 41 da LGPD, torna-se extremamente difícil e custoso para as empresas de pequeno porte o cumprimento da lei. Na avaliação da Confederação Nacional da Indústria[49], "a obrigatoriedade de manter registro das operações

[49] Disponível em: <https://noticias.portaldaindustria.com.br/noticias/leis-e-normas/estudo-da-cni-reforca-importancia-de-tratamento-diferenciado-na-lgpd-para-microempresas/>. Acesso em 22 fev. 2021.

	de tratamento de dados e a nomeação de um encarregado, uma espécie de ouvidor da LGPD é incompatível com a realidade das empresas de menor porte." É importante considerar que pequenas empresas podem movimentar grande volume de dados pessoais ou até mesmo de dados sensíveis. A título de exemplo, diversas são as startups de serviços de saúde[50], cujos serviços envolvem o tratamento de dados sensíveis, os quais possuem maior proteção da legislação brasileira em razão do seu potencial discriminatório. Assim, é recomendável que a regulamentação não exclua agentes de tratamento baseados somente em seu tamanho ou faturamento, mas sim aqueles cujo tratamento de dados não gere riscos aos direitos e liberdades dos titulares, de forma a calibrar a regulamentação, já que a dispensa da obrigação de nomear o encarregado às pequenas empresas não as exime do cumprimento da LGPD, mas apenas exclui a obrigação de profissional (ou equipe) destacada para a função. É possível, portanto, através da regulamentação, exigir o cumprimento das atribuições diretamente pelo agente de tratamento, o que torna a adequação à LGPD menos custosa e possível de ser executada, sem reduzir a proteção aos direitos dos titulares.

[50] Disponível em: <https://vocesa.abril.com.br/mercado/o-crescimento-das-startups-de-saude-no-brasil/>. Acesso em 22 fev. 2021.

	Sugere-se um balanceamento na regulamentação da dispensa do encarregado entre pequenas empresas que não tratem dados pessoais em larga escala, ou ainda, que seus negócios não sejam baseados em tratamento de dados sensíveis. A exemplo, o GDPR, em seu artigo 37, exige a indicação do *Data Protection Officer* (figura correspondente ao encarregado, na lei brasileira), apenas em alguns casos, quais sejam: (i) tratamento de dados realizado por entidade do Poder Público; (ii) as principais atividades empresariais do agente de tratamento envolvem tratamento de dados que, por sua natureza, escopo ou finalidade, requerem monitoramento sistemático e regular dos titulares de dados em larga escala; ou (iii) as atividades empresariais requerem tratamento de dados sensíveis em larga escala ou dados relacionados a condenações ou infrações criminais. Vê-se que a União Europeia adotou o critério do risco em relação ao tipo do agente de tratamento (poder público), ao volume ou tipos de dados tratados para a dispensa da figura equivalente ao encarregado, e não do tamanho da empresa agente de tratamento.

	Por outro lado, a legislação australiana não exige a indicação da figura equivalente ao encarregado, mas é considerada uma boa prática[51].
Quais são os impactos da elaboração do relatório de impacto à proteção de dados pessoais aos agentes de pequeno porte?	Conforme o disposto no art. 5º, VII, da LGPD, **relatório de impacto** é a documentação **do controlador** que contém a descrição dos processos de **tratamento** de dados pessoais **que podem gerar riscos às liberdades civis e aos aos direitos fundamentais**, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Ou seja, a produção deste relatório está diretamente relacionada à avaliação de riscos periódica que deve ser desempenhada pelo controlador no âmbito do seu programa de governança de dados, porque a obrigação só diz respeito aos tratamentos que podem gerar algum risco. Nesse sentido, a documentação dos impactos de um tratamento também é necessária quando esse processamento é baseado no legítimo interesse, resguardados os segredos comercial e industrial (art. 10, §3º, LGPD), então é necessário que a empresa tenha realizado o mapeamento dos fluxos de dados para definir quais tratamentos estão fundamentados nessa base legal. Sobre esse ponto, ainda se mostra crucial o desenvolvimento sobre o teste de proporcionalidade que deve ser realizado para garantir que o legítimo interesse é adequado, uma vez que devem prevalecer os direitos e liberdades fundamentais do titular (art. 7º, IX, LGPD).

[51] Disponível em <https://www.linklaters.com/pt-br/insights/data-protected/data-protected---australia>. Acesso em 23 fev. 2021.

	Diante disso, é inegável que tal atividade gerará impactos financeiros às empresas e também poderá gerar mudanças no modo de realização de algumas operações desempenhadas pela organização. Contudo, esse documento facilitará o desenvolvimento do relacionamento e diálogo entre o controlador e a ANPD. Ainda no art. 10, §3º, da LGPD, está previsto que a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais quando determinado tratamento tiver como fundamento o legítimo interesse. Dessa forma, a ANPD deve definir se essa solicitação também poderá ser direcionada a empreendimentos de pequeno porte. Se sim, é fundamental garantir que não haja o esvaziamento da base legal dos interesses legítimos do controlador para as empresas de pequeno porte, principalmente ao se considerar que essa base amplia as possibilidades de tratamento e pode ser um diferencial competitivo. Sobre os efeitos positivos, acreditamos que tal documentação será compreendida como boa prática pela ANPD, principalmente se tais relatórios contarem com as medidas de mitigação de risco adotadas pela empresa. Nesse sentido, a própria LGPD traz como parte do programa de governança em privacidade, uma boa prática, o estabelecimento de políticas e salvaguardas a partir do processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, I, d). Então, o relatório de impactos será

	uma importante forma de prestação de contas perante à ANPD e à sociedade sobre o *compliance* das companhias.
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?	Haja vista a redação do art. 14 da LGPD, quanto ao tratamento de dados pessoais de crianças e adolescentes, há quem entenda que a base legal do consentimento prevalece de forma obrigatória sobre as demais. Entretanto, o cenário que se apresenta é de um cenário com cada vez maior desconfiança no consentimento[52]. Por isso, considerando os posicionamentos do Comitê sobre os Direitos da Criança sobre a interpretação de disposições jurídicas abertas, como é o caso do art. 14[53], o LAPIN sugere que o melhor entendimento seja o de que outras bases legais devem sim ser aplicáveis para o tratamento de dados de crianças e de adolescentes, desde que observado o melhor interesse do menor e que seja feita uma análise razoável sobre os impactos da aplicação dessas disposições. Por isso, considerando esse princípio interpretativo, acredita-se que o legítimo interesse e a proteção de crédito não são aplicáveis para o tratamento de dados de crianças e adolescentes, considerando, por um lado, a excessiva

[52] MENDES, L. S.; FONSECA, G. C. S. **Proteção de Dados para Além do Consentimento: tendências contemporâneas de materialização.** Rev. Estudos Institucionais, v. 6, n. 2, p. 508-533, maio/ago 2020.

[53] "Como princípio jurídico fundamentalmente interpretativo, de acordo com o Comitê, significa que **se uma disposição jurídica estiver aberta a mais do que uma interpretação, deve ser escolhida a que efetivamente melhor satisfaça o melhor interesse da criança**. Por fim, como regra de procedimento, sempre que é tomada uma decisão que afeta uma determinada criança, um grupo de crianças ou as crianças em geral, o processo de tomada de decisão deve incluir uma avaliação de seu possível impacto - regra de onde se poderia tirar, por exemplo, a obrigação de se elaborar Relatórios de Impacto à Proteção de Dados Pessoais quando dados de crianças e adolescentes são tratados." FERNANDES, E. R. **Crianças e adolescentes na LGPD: Bases legais aplicáveis.** Migalhas. Outubro de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/335550/criancas-e-adolescentes-na-lgpd--bases-legais-aplicaveis>. Acesso em 01 mar. 2021.

	amplitude da base do legítimo interesse, e pelo fato de que não é concedido crédito a esse grupo etário, o que esgota a aplicação desse comando[54]. O mesmo vale para os dados sensíveis referentes aos menores. As bases legais mais restritivas previstas no art. 11 da LGPD também podem embasar o tratamento, desde que o melhor interesse do menor seja observado. Nesses casos, poderia a ANPD ainda trazer uma categorização de dados hipersensíveis desses indivíduos que não poderiam ser tratados, como dados sensíveis relacionados à biometria de crianças, por exemplo. Tal matéria ainda precisaria de regulamentação específica[55], mas garantiria uma maior proteção das informações desse grupo social. Diante do exposto, o LAPIN acredita que o consentimento deve ser a base legal prioritária para o tratamento de dados de crianças e adolescentes, a partir da observância do art. 14, mas não a única, cabendo regulamentação específica sobre quais outras bases, seja para dados sensíveis ou não,previstas nos art. 7º e 11 podem ser utilizadas, desde que com a observância do melhor interesse do titular (as crianças ou os adolescentes).

[54] Ibid.
[55] Id.

	Contudo, caso a ANPD entenda pela primeira corrente interpretativa, em que o consentimento prevaleça de forma obrigatória sobre as outras bases legais, é importante ressaltar que a utilização dessa base legal exige a adequada gestão, por parte do controlador, de todo o ciclo de governança dos dados, de modo a garantir seu tratamento de acordo com o estipulado nos princípios e direitos previstos na LGPD, conforme se verifica no tópico seguinte. Tal funcionamento pressupõe obrigações ao controlador que demandam esforço, que pode ser considerado desproporcional, a ser imposto às empresas de pequeno porte. Independentemente do entendimento sobre as bases legais aplicáveis ao tratamento de dados de crianças e adolescentes, e ainda, considerando o questionamento quanto ao tratamento de dados sensíveis, o LAPIN entende que os impactos na implementação para empresas de pequeno porte são os mesmos da implementação do programa de governança de dados, conforme tópico seguinte, pois é através deste que as empresas podem alcançar a conformidade com a LGPD. A regulamentação de exceções às obrigações impostas às pequenas empresas em relação ao tratamento de dados sensíveis ou de crianças e adolescentes devem ser observadas com cautela, já que a LGPD buscou claramente trazer uma maior proteção a estes titulares. Inclusive, o art. 37 da LGPD traz como obrigação geral o registro das operações de tratamento de dados pessoais, especialmente quando

	baseado no legítimo interesse. Dessa forma, considerando a sensibilidade dos dados de crianças e adolescentes, a ANPD pode trazer uma obrigação como essa para o tratamento de tais dados.
Quais são os impactos da implementação do programa de governança de dados aos agentes de pequeno porte?	Os impactos da implementação do tratamento de dados pelos agentes de tratamento empresas de pequeno porte são diversos, tendo em vista o cumprimento dos requisitos legais e estabelecimento de procedimentos internos para a governança dos dados. O primeiro passo para a governança de dados pessoais consiste em averiguar a existência dos impactos por meio do mapeamento de todas as operações de tratamento de dados pessoais abarcadas pelas atividades empresariais, para cumprir a obrigação estabelecida no art. 37 da LGPD, de manter registro das operações de tratamento de dados. *"Importante salientar que o controlador deverá manter os registros de operações de tratamento de dados pessoais devidamente atualizados, de modo que a empresa deverá criar, em seus processos, todo um mecanismo de registro de novas operações de tratamento de dados pessoais, ou mesmo das antigas,*

	quando modificadas. Há que se criar uma verdadeira cultura dentro da empresa, para manutenção desses registros devidamente atualizados."[56] Em relação ao registro de operações de tratamento, a LGPD não delimita os requisitos mínimos de tal obrigação como faz o art. 30 do GDPR, o qual estabelece os itens mínimos que devem constar do inventário de dados. A exemplo da União Europeia, sugere-se a regulamentação, pela ANPD, sobre os itens essenciais que deverão constar nos registros das operações de tratamento de dados pessoais, para que as organizações possam atuar com segurança jurídica. Tal regulamentação também visa otimizar o serviço público, eis que, em fiscalizações, não é adequado que a ANPD receba informações em excesso provenientes de registros de operações de tratamento de dados, mas apenas aquelas realmente úteis para avaliar o impacto das atividades à proteção de dados pessoais. Ademais, exceções (de itens essenciais ou da realização do próprio registro) podem ser consideradas na regulamentação da LGPD para os agentes de tratamento que sejam empresas de

[56] MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev. atual. e ampli. São Paulo: Thomson Reuters Brasil, 2019. p. 311.

	pequeno porte, considerando tipo de atividade empresarial, tamanho da empresa e baixo risco de atividades em relação aos direitos dos titulares. O GDPR também isenta alguns tipos de agentes da obrigação de registro de operações de tratamento[57]. Porém, essa isenção não é absoluta, segundo entendimento do *Working Party* 29 (WP29) em *Position Paper*[58] referendado pelo *European Data Protection Board* (EDPB). A isenção não se aplica, por exemplo, aos tratamentos de dados que: (i) tenham probabilidade de resultar em risco para os direitos e liberdades dos titulares de dados; ou (ii) não sejam ocasionais; ou (iii) incluam dados sensíveis ou dados pessoais relacionados a condenações criminais e infrações. Ademais, o mesmo relatório do WP29 destaca que o registro das operações de tratamento de dados é muito útil para suportar a análise das implicações de qualquer tratamento de dados, seja existente ou planejado. Isso também se verifica na legislação brasileira. Mapeadas as operações de tratamento de dados pessoais, a organização terá melhores condições de efetuar a adequada gestão dos dados para o

[57] Art. 30 (5) GDPR - "As obrigações a que se referem os n.os 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10."

[58] Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045>. Acesso em 20 fev. 2021.

	cumprimento de outras obrigações da LGPD, tais como: (i) gestão do consentimento conforme art. 8º da LGPD, que envolve a coleta (forma), o armazenamento (forma e prazo), e as formas de atendimento da revogação; (ii) análise sobre as operações de tratamento baseadas em legítimo interesse, para verificar se estão de acordo com os requisitos do art. 10 da LGPD; e (iii) elaboração de fluxos internos para garantir o atendimento de direitos aos titulares, na forma do art. 18 da LGPD. O atendimento de direitos dos titulares, obrigação imposta pela LGPD aos controladores, possui vários desdobramentos nas atividades internas dos agentes de tratamento, como: (i) forma de recebimento de solicitação de exercício de direitos; (ii) comprovação da identidade do titular que solicita exercício de direitos; (iii) criação de fluxos internos contendo responsáveis e prazos para a coleta das informações solicitadas pelo titular; (iv) análise sobre a viabilidade de atendimento do direito, como por exemplo, a eliminação de dados; (v) solicitação de informações a outros agentes de tratamento, como operador e co-controlador; e (vi) forma de resposta ao titular. Flexibilizações quanto aos direitos dos titulares também podem ser consideradas às empresas de pequeno porte, como, por exemplo, o alargamento do prazo para o atendimento de direitos ao titular (ainda pendente de regulamentação por esta Autoridade).

	Portanto, nota-se que a implementação de um programa de governança de dados pessoais para fins de cumprimento da LGPD gera vários novos procedimentos e fluxos internos, os quais podem ser de difícil cumprimento para agentes de tratamento que sejam empresas de pequeno porte, o que merece ser objeto de regulamentação diferenciada por parte desta Autoridade. Vale ressaltar que a regulamentação de forma diferenciada não deve significar o aumento de risco ou a redução de direitos dos titulares, já que categorias especiais, como dados sensíveis ou dados de crianças e adolescentes, podem ser isentas de regulamentação diferenciada, conforme legislações internacionais apontadas.
Quais são os impactos da implantação de política de segurança relativa à proteção de dados pessoais aos agentes de pequeno porte?	O art. 46 da LGPD estabelece que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", estipulando a obrigação de implantação de política de segurança relativa à proteção de dados pessoais. A segurança da informação é essencial ao funcionamento de uma empresa e à manutenção de sua reputação, principalmente considerando a informação como um ativo econômico. A LGPD surge com o intuito de trazer maior segurança aos tratamentos de dados realizados, dando maior controle ao titular,

	mas sem impossibilitar o fluxo de dados. Ou seja, a arquitetura de proteção de dados deve alinhar as regras de privacidade e segurança com a era da economia de dados, que depende do tratamento desses ativos. Surge, então, a necessidade das organizações (públicas e privadas) adotarem programas de adequação para garantir a observância das normas protetivas. Contudo, o *compliance* de privacidade, proteção de dados e segurança da informação gera diversos custos às organizações, o que pode ser um empecilho para empresas com faturamento limitado, como as empresas de pequeno porte, e para as iniciativas que dependem de grande investimento em pesquisa e desenvolvimento (P&D), como as *startups* e as empresas de inovação[59]. Prova disso é o fato de que quanto maior o porte, mais as medidas de proteção de dados estão presentes nas empresas; contudo, 23% das microempresas brasileiras e 13% das empresas de pequeno porte confirmarem que não têm, mas preveem investimento nessas medidas para o futuro, o que demonstra a intenção dessas em se adequar aos processos necessários para a segurança da informação[60].

[59] Em 2017, somente 32% das pequenas e médias empresas na Argentina realizaram algum tipo de investimento, considerando inclusive capacitações ou contratação de consultorias. As empresas que fizeram tais investimentos tiveram maiores níveis de produtividade, o que justifica a imposição de incentivos e flexibilizações pelo Estado.
UCEMA. **Gobierno corporativo em micro, pequenas y medianas empresas de Argentina**. Buenos Aires, Argentina, 2020. Disponível em: < https://ucema.edu.ar/publicaciones/doc_trabajo.php>. Acesso 20 fev. 2021.

[60] SERASA EXPERIAN. **Como as empresas se preparam para atender à nova regulamentação.** 2020. Disponível em: <https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf>. Acesso 01 mar. 2021.

	Esse gasto se torna ainda mais evidente quando se considera a necessidade de investir em componentes humanos, em destaque a obrigação de indicação de encarregado, o que traz gastos contínuos às organizações. Além disso, devem ser consideradas a necessidade de capacitação e engajamento do componente humano das empresas, o que também gera impactos financeiros. Ressalta-se que alguns modelos de negócio, como o MEI, não possuem funcionários internos para suprir a necessidade de força de trabalho humana para ocupar todos os papéis indicados pela LGPD. Então, para o preenchimento dessas posições, algumas empresas irão buscar pessoas ou serviços externos à organização para cumprir com as obrigações legais relacionadas à arquitetura de segurança de dados. Além disso, a ação humana deve estar conjugada com a adoção de medidas técnicas de segurança, o que também pode gerar grande impacto financeiro, principalmente para organizações que lidam com altos níveis de tratamento de dados. Como exemplo, existem as regras internacionais estabelecidas sobre o tema, como o ISO 27001 e o ISO 27002, que estabelecem uma série de medidas para garantir a segurança da informação (p. ex.: auditorias, monitoramento, criação de comitê de gestão da informação, entre outras) que devem ser adaptadas à realidade das empresas de pequeno porte.

	É uma boa prática que todas as medidas de segurança adotadas por uma organização estejam documentadas em uma "Política de Segurança" ou documento semelhante. Ela deve explorar desde questões relacionadas ao *privacy by design* até o término do tratamento dos dados pessoais, podendo dissertar inclusive sobre a forma de comunicação de incidentes de segurança. É aconselhável que as políticas da empresa estejam disponíveis ao público, em especial aos titulares dos dados, a fim de observância do princípio da prestação de contas e transparência. Diante disso, a empresa de pequeno porte buscará formas de atender essas medidas de boas práticas, para que os efeitos positivos do *compliance* de privacidade sejam alcançados. Mas, para tanto, se mostra necessário o auxílio da ANPD, com disponibilização de templates, guias de boas práticas, painéis interativos, etc. Mostra-se necessário que todas as empresas que realizam tratamento de dados façam uma avaliação dos riscos das suas atividades para questões relacionadas à segurança. Essa nos parece ser a melhor forma de considerar quais serão as organizações obrigadas a implantar políticas de segurança e quais deverão adotar salvaguardas adicionais ou medidas mais sofisticadas. Há impactos relacionados, também, sobre a forma de documentação dessa avaliação.

	De qualquer forma, as organizações deverão adotar medidas essenciais para a segurança da informação, quais sejam: confidencialidade (por meio de controles de acesso, por exemplo)[61]; integridade dos dados; e disponibilidade dos dados[62], inclusive de acordo com as regras já estabelecidas internacionalmente sobre a segurança da informação (como as já citadas, ISO 27001 e ISO 27002). Para tanto, é necessário explorar e oferecer opções para garantir a segurança da informação, mas que não gerem tantas repercussões financeiras às organizações. Uma das opções é a adoção e divulgação de manuais de segurança[63], nos termos das normas técnicas já mencionadas, mas direcionados para as realidades dos agentes de pequeno porte. Isso poderia ser feito diretamente pelas empresas, por associações ou pela ANPD (art. 46, §1º, LGPD). Também é necessário entender em qual momento do ciclo do dado o agente de pequeno porte irá atuar - podendo participar de tratamento de dados em parceria com empresa de grande porte, o que pode modificar a situação da organização. Isso porque o art. 47 da LGPD dispõe que qualquer pessoa que

[61] HANSEN, M. *et al*. **Protection goals for privacy engineering**. International Workshop on Privacy Engineering. Maio de 2015. Disponível em: <https://www.ieee-security.org/TC/SPW2015/IWPE/2.pdf>. Acesso em 01 mar. 2021.

[62] GUAMÁN, C. R. S. *et al*. **Percepción de Seguridad de La Información en las Pequeñas y Medianas Empresas en Santo Domingo**. Rev. Investigación Operacional. Vol. 40, n. 3, 421-428. 2019.

[63] No estudo já mencionado de GUAMÁN, resta demonstrado que a maioria das pequenas e médias de Santo Domingo empresas contam com documentos que determinam as intenções, alcance, objetivos, responsabilidades, políticas e diretrizes da política da segurança da informação, o que comprova o baixo impacto dessa medida. GUAMÁN, C. R. S. *et al*. **Percepción de Seguridad de La Información en las Pequeñas y Medianas Empresas en Santo Domingo**. Rev. Investigacion Operacional. Vol. 40, n. 3, 421-428. 2019.

	intervenha em uma das fases do tratamento de dados se obriga a garantir a segurança da informação. Então deve-se considerar a eventualidade do tratamento de maior risco para serem definidas as medidas realmente obrigatórias a serem adotadas pela organização. Por fim, há também o impacto oriundo da necessidade de revisão periódica, o que gera necessidade de aplicação de melhorias e correções (ver tópico seguinte). De qualquer forma, a adoção de política de segurança evitará incidentes de segurança, o que é um efeito positivo tanto para os titulares quanto para o controlador, que está submetido a possíveis sanções. Além disso, ao adotar política de segurança, caso ocorra algum incidente, o controlador poderá ter as sanções mitigadas.
Quais são os impactos da implantação de avaliação sistemática de riscos à privacidade dos dados aos agentes de pequeno porte?	Vários impactos relacionados à implementação de avaliação sistemática de riscos à privacidade se relacionam aos pontos já apresentados de necessidade de contratação de pessoal qualificado para realização de tais avaliações, implementação de sistema de segurança da informação, promoção de um programa de governança de dados, etc. De qualquer forma, a LGPD, assim como o GDPR, adotou um sistema de avaliação de riscos para definir ou mitigar várias atribuições aos agentes de tratamento. Essa abordagem segue um processo contínuo e permanente, devendo ser reavaliado de tempos em tempos. É necessário que a ANPD (ou outros agentes do sistema) defina qual seria a periodicidade razoável para refazer a avaliação de riscos à

	privacidade, de forma que os agentes de tratamento consigam mensurar de forma mais precisa os impactos dessa avaliação. Ressalta-se que, inicialmente, haverá significativo impacto financeiro e de mudanças de atividades para que as organizações se adequem às novas regras de proteção de dados. Contudo, a tendência é de que os investimentos para a adequação da organização diminuam com o passar do tempo, porque o processo de revisão tende a ser mais simples em comparação ao de implementação. Mas será esse processo que possibilitará às organizações que se isentem de determinadas obrigações, uma vez que alguns tratamentos de baixo risco podem ser excluídos do escopo da lei e, no mesmo sentido, a obrigação de comunicação de incidente de segurança à ANPD também só diz respeito a fatos que possam acarretar risco ou dano relevante aos titulares, o que também será verificado através da avaliação de riscos (art. 48, LGPD). Outro impacto será a necessidade de documentação de tais avaliações sistemáticas. Inclusive para observar o princípio da transparência, é uma boa prática a documentação das análises de riscos à privacidade realizadas por uma organização. É relevante definir como tal documentação deve ser realizada e também o tempo de preservação de tais documentos, devendo a ANPD definir requisitos mínimos para a confecção do documento.

	Por fim, é a partir dessa avaliação que as organizações alcançarão conclusões sobre os tratamentos de dados realizados por elas, inclusive podendo concluir que a melhor solução seria o término de determinado tratamento. Portanto, um possível impacto é a mudança de determinadas atividades realizadas por empresas de pequeno porte a fim de garantir a segurança da informação.
Quais são os impactos da implantação da portabilidade de dados pessoais aos agentes de pequeno porte?	A portabilidade de dados pessoais é classificada como um direito do titular de dados, conforme o art. 18 da LGPD. O principal impacto relacionado ao direito da portabilidade diz respeito às regras de interoperabilidade que serão definidas pela ANPD (art. 40, LGPD). Deve-se estabelecer se as empresas de pequeno porte deverão respeitar os padrões de interoperabilidade e se deverão arcar com as despesas relacionadas a isso. Ainda sobre a operacionalização desse direito, a LGPD fala que o exercício da portabilidade depende da requisição expressa do titular. Dessa forma, as empresas de pequeno porte também devem se adequar para receber tais solicitações e atendê-las em um prazo razoável. A implementação de uma plataforma de portabilidade, por exemplo, pode ser extremamente custosa, especialmente para empresas que realizam tratamentos complexos, inclusive para o processo de anonimização dos dados. Essa plataforma deve oferecer a possibilidade de o titular diretamente solicitar a portabilidade dos seus dados, devendo a ANPD definir se essa requisição será atendida

	somente com a transferência de tais dados para outro fornecedor ou se será possível que tal pedido seja concluído com a disponibilização em formato de documento para o titular. De qualquer forma, a própria LGPD já traz um limite para o direito à portabilidade de dados: a observância dos segredos comercial e industrial. Por isso, também é necessário que seja regulamentado o que será considerado como segredo empresarial - não há definições se dados gerados a partir de inteligência artificial devem ou não participar do processo de portabilidade de dados, porque esse processo de IA pode estar protegido pelo segredo industrial. Além disso, é necessário considerar que a portabilidade pode ser uma importante forma de garantir a entrada de novos *players* no mercado, principalmente em mercados digitais monopolizados, diminuindo custos de troca e diminuindo os efeitos de rede relacionados a esses mercados. Dessa forma, a portabilidade trará impactos positivos aos agentes de pequeno porte, principalmente aqueles novos agentes que ainda estão se consolidando nos mercados.
Qual instrumento regulatório poderia ser utilizado para promover e incentivar a inovação	A Autoridade pode se valer do chamado *sandbox* regulatório, uma nova abordagem regulatória que objetiva o desenvolvimento e testagem de novos produtos e serviços inovadores com a supervisão da

nos agentes de pequeno porte?	ANPD, acarretando em benefícios para as organizações e para a Autoridade, na medida em que, dentre outros pontos[64]: ● Incentiva a inovação das PMEs com maior confiança sobre o ambiente regulatório; ● Reduz as incertezas regulatórias; ● Melhora a eficácia da Autoridade porquanto é uma regulação responsiva focada em resultados; e ● Há razoável garantia de que produtos inovadores estarão em conformidade com a lei de proteção de dados. Além deste instrumento regulatório pensado especificamente para a promoção de incentivo da inovação, a ANPD também poderá, quando da normatização das demais regulamentações dos pontos ainda em aberto na LGPD, sempre levar as características e especificidades das PMEs e startups em consideração, por exemplo, quando a Autoridade regular o direito à portabilidade de dados e o direito de revisão de decisões automatizadas, criando mecanismos simplificados e inovadores para a conformidade com a lei.

[64] CENTRE FOR INFORMATION POLICY LEADERSHIP. **Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice**. CIPL, 8 mar. 2019. Disponível em: < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf>. Acesso em 22 fev. 2021.

	Ademais, outros instrumentos regulatórios podem ser adotados pela Autoridade para alavancar a inovação no país, como a ratificação e validação de boas práticas elaboradas por associações representativas de setores da economia, por exemplo, a autorregulação setorial e guias de boas práticas elaborados por Confederações Nacionais.

LAPIN
LABORATÓRIO DE POLÍTICAS PUBLICAS E INTERNET

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx
Art. Xxxx

ANEXO I

Descrição detalhada das atividades realizadas pelas Autoridades Europeias de Proteção de Dados para que agentes de tratamento de dados de pequeno porte estejam em conformidade com o GDPR

País	Ações
Alemanha[65]	· Aconselhamento individual permanente para controladores, operadores e DPOs de PMEs, incluindo startups; · Participação em eventos de treinamento, seminários e workshops como palestrantes, com o objetivo de apoiar PMEs na implementação e monitoramento de conformidade com o GDPR; · Publicação de diversos materiais de orientação e perguntas e respostas destinadas às PME.

[65] EDPB, **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf> p. 37 . Acesso em: 22 fev.2021.

Áustria[66]	· Campanhas anuais de conscientização; · Apresentações e palestras para diversos públicos; · Publicação de material de orientação e FAQ; · Participação em conferências; · Adoção de *whitelist* para tratamentos de dados pessoais isentos de relatório de impacto de proteção de dados 'DPIA).

[66] Ibid, p. 36; The Legal Information System of the Republic of Austria, **Exceções à avaliação de impacto de proteção de dados**. Disponível em: <www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdfsig>. Acesso em: 22 fev. 2021.

Bélgica[67]	· GDPR *vade-mecum* para PMEs; · Relatório sobre a implementação do GDPR em PMEs; · Relatório sobre conhecimento e compreensão do GDPR por PMEs; · Guia de perguntas frequentes para PMEs sobre conformidade com o GDPR, com exemplos práticos; · Consulta em grande escala sobre PMEs para identificar suas necessidades em relação à conformidade com o GDPR; · Janeiro de 2020: Atuação no The BOOST-project (cofinanciado pela CE) que pretende produzir orientações e ferramentas para os temas (i) princípio da transparência, (ii) DPIA e (iii) conceitos de *controlador* e *operador*. • Como parte do projeto BOOST, as PMEs recebem uma *newsletter* bimestral.

[67] EDPB (n. 58), p. 36; Autorité de protection de données, **PME**. Disponível em: <www.autoriteprotectiondonnees.be/professionnel/chercher?q=PME&s=&l=25>. Acesso em 22 fev. 2021.

Bulgária[68]	· Linha direta permanente para consulta e aconselhamento; · Projeto SMEDATA II (cofinanciado pela CE) cujo objetivo é garantir a aplicação efetiva do GDPR através da sensibilização, formação e capacitação para PMEs e profissionais do direito. A duração do projeto é de 18 meses a partir de 01/01/2021. Resumo das ações concretas: • Pesquisas sobre os desafios enfrentados pelas PMEs e suas associações durante a implementação do GDPR (pesquisas 1 e 2); • 13 eventos de treinamento para mais de 800 representantes de PMEs em 8 cidades búlgaras em setembro e outubro de 2019; • *GDPR In Your Pocket* - aplicativo móvel; • Conferência internacional *SME Challenges and GDPR* para mais de 170 participantes em novembro de 2019; • *Self-Assessment and Awareness Tool.*

[68] EDPB (n. 58) p. 36; SMEDATA II, **Ensuring the Highest Degree of Privacy and Personal Data Protection through Innovative Tools for SMEs and Citizens**. Disponível em: <https://smedata.eu/index.php/project/overview/>. Acesso em 22 fev. 2021.

Chipre[69]	· Orientações escritas (p. ex., em relação a videomonitoramento em restaurantes ou uso de sistemas biométricos em academias); · Oficinas personalizadas para setores específicos; · Apresentações, palestras em universidades e em associações profissionais de diversos setores.

[69] EDPB (n. 58) p. 36.

Croácia[70]	· Cooperação com o setor público e privado a fim de aumentar a conscientização sobre a proteção de dados pessoais, incluindo seminários, workshops e conferências; · *Blacklist* elencado de maneira não exaustiva situações que exigem o DPIA; · Implementação do projeto *ARC-Awareness Raising Campaign for SMEs*, em cooperação com as Autoridades Irlandesa e Belga e cofinanciado pela CE, com duração de 24 meses a partir de março de 2020. Os principais objetivos do projeto envolvem (i) sensibilizar as PMEs sobre as obrigações do GDPR; (ii) ajudar as PMEs a cumprirem essas obrigações; e (iii) esclarecer dúvidas sobre implementação do GDPR; • Esses objetivos serão alcançados por meio das seguintes atividades: (i) realização de pesquisa para identificar as necessidades das PMEs; (ii) preparação de materiais educacionais sobre o GDPR; (iii) organização de consultas nos principais centros regionais da Croácia, onde PMEs poderão receber apoio direto para solucionar problemas específicos; (iv) organização de conferências internacionais para troca de experiências e apresentação de melhores práticas; e (v) publicações dos resultados do projeto.

[70] EDPB (n. 58) p. 38; EDPB, **List of the types of processing for which a DPIA shall be required pursuant to Article 35.4**. Disponível em: <https://edpb.europa.eu/sites/edpb/files/decisions/list_of_the_types_of_processing_for_dpia_croatia_35_4.pdf>. Acesso em: 22 fev. 2021.

Dinamarca[71]	· Desenvolvimento do guia interativo *Privacy Compass* visando auxiliar PMEs a estarem em conformidade com o GDPR; · Participação em conferências e eventos voltados às PMEs; · Publicação de informação específicas às PME em seu site; · Linha direta para consulta e aconselhamento; · Podcasts com tópicos focados em PMEs; · *Checklists*, FAQ e *guidelines*.
Eslováquia[72]	· Participação em seminários, workshops, conferências e palestras para SMEs; · Orientação às PMEs por e-mail.

[71] EDPB (n. 58) p. 37; Danish Portal for Business (VIRK), **Privacy Compass**. Disponível em: <https://startvaekst.virk.dk/privacykompasset/om-privacykompasset>. Acesso em 22 fev. 2021.
[72] EDPB (n. 58) p. 44.

Eslovênia[73]	· Elaboração de guidelines, infográficos, e participação em palestras, algumas em parceria com a Câmara de Comércio e Indústria da Eslovênia; · Desenvolvimento do projeto RAPiD.si (cofinanciado pela CE) com foco na educação e orientação às PMEs. Foi criado um site específico com, por exemplo, quiz interativo, FAQ, modelos de formulários e notícias recentes.
Espanha[74]	· Linha direta para consulta e aconselhamento para controladores e operadores; · Consulta com PMEs sobre o principal impacto do GDPR; · Orientações, guias e ferramentas destinadas a apoiar as PMEs na adequação ao GDPR; • Exemplo de ferramenta: FACILITA RGPD, que é um questionário online onde empresas e profissionais podem verificar por meio de uma série de perguntas se as operações de tratamento de

[73] EDPB (n. 58), p. 44; Information Commissioner, **Raising Awareness on Data Protection and the GDPR in Slovenia - RAPiD.Si project**. Disponível em: <www.ip-rs.si/en/data-protection/projects/>. Acesso em: 22 fev. 2021; Information Commissioner, **Protection of Personal Data - Website to help small and medium-sized businesses**. Disponível em: <https://upravljavec.si/>. Acesso em: 22 fev. 2021.
[74] EDPB (n. 58), p. 37.

	dados que realizam podem ser consideradas de baixo risco, obtendo, ao final do teste, os documentos mínimos para facilitar a aplicação do GDPR.
Estônia[75]	· Orientações, consultas e treinamentos em parceria com diferentes associações profissionais; · Linha direta para consulta e aconselhamento; · Atuação para desenvolvimento de mais treinamentos para DPOs pelas principais universidades na Estônia.
Finlândia[76]	· Materiais de orientação e feedback a setores específicos; · Organização de seminários e participação como palestrante; · Linha direta para consulta e aconselhamento. · Envio de *newsletter* mensal;

[75] Ibid.
[76] Ibid, p. 38; Office of the Data Protection Ombudsman, **Data protection opening doors into Europe for SMEs - GDPR2DSM**. Disponível em: <https://tietosuoja.fi/en/-/data-protection-opening-doors-into-europe-for-smes>. Acesso em: 22 fev. 2021.

	· Atuação no projeto GDPR2DSM (cofinanciado pela CE) que visa fornecer às microempresas e PMEs informações e ferramentas para garantir uma proteção de dados eficaz.
França[77]	· Pacote dedicado às PMEs disponível no site da CNIL, incluindo um guia prático; · Publicação de vídeo com um Youtuber sobre como aplicar o GDPR (destinado ao público em geral); · Registro das operações de tratamento de dados pessoais simplificado; · Treinamento online: *The GDPR Workshop*; · Conteúdo específico sobre segurança e dados pessoais; · Outras ferramentas amplamente utilizadas por PMEs: ● Linha direta para consultas; ● FAQ; ● *Software* para ajudar na elaboração do DPIA;

[77] EDPB (n. 58), p. 38.

	• *Whitelist* para operações de tratamento de dados pessoais isentos do DPIA; • Formulário de notificação de incidente de segurança.
Holanda[78]	· Campanha de informação sobre o GDPR para organizações e o público em geral; · Campanhas dirigidas a PMEs; · Participação em eventos, entrevistas, publicação de informações em redes sociais e de vídeos sobre privacidade; · Guias para realização do DPIA.
Hungria[79]	· Guias para SMEs;

[78] Ibid, p. 42; Autoriteit Persoonsgegevens, **Data protection impact assessment (DPIA)**. Disponível em: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia>. Acesso em: 22 fev. 2021.
[79] EDPB (n. 58), p. 39; Trilateral Research, **STAR II - SupporT small And medium enterprises on the data protection Reform II**. Disponível em: <https://www.trilateralresearch.com/work/star-ii/>. Acesso em: 22 fev. 2021.

	· Atuação no Projeto *Star II* (*Support Small and Medium Enterprises on the Data Protection Reform II*), cofinanciado pela CE, que tem como objetivos a promoção de campanhas de conscientização, o estabelecimento de uma linha direta, e a publicação de *guidelines* e pesquisas.
Irlanda[80]	· Iniciativa conjunta com a Autoridade Croata (projeto ARC descrito acima); · Publicação de orientações no site.
Islândia[81]	· Palestras, conferências e presença na *UTmassen* (maior conferência de tecnologia da Islândia); · Publicação de orientações; · Q&A para organizações e titulares de dados; · Balcão de atendimento para PMEs e autoridades locais, onde foram esclarecidas dúvidas sobre a implementação do GDPR (serviço ficou disponível por 13 meses – foi encerrado em 2019).

[80] EDPB (n. 58), p. 39.
[81] Ibid.

Itália[82]	· Elaboração de guidelines; · Atuação no projeto SMEDATA (detalhes acima, em *Bulgária*). Ações concretas: • 12 eventos regionais de sensibilização para PMEs e profissionais do Direito; • 2 eventos relativos a uma ferramenta *self-assessment* de sensibilização com base nas necessidades e processos específicos das PMEs (presença de mais de 60 representantes de universidade, associações comerciais e empresas associadas); • Condução de treinamentos.

[82] Ibid, p. 40; Garante per la protezione dei dati personali, **Practical Guidelines and Simplifying Measures for SMEs**. Disponível em: <www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1435985>. Acesso em: 22 fev. 2021.

Letônia[83]	· Atuação no projeto DPSME, cofinanciado pela CE. O projeto, que durou 24 meses e foi encerrado em novembro de 2020, teve como objetivo melhorar a preparação das PMEs para aplicação do GDPR; · Participação em seminários, workshops e conferências; · Consultas por telefone e presenciais; · Guia de Tratamento de Dados para PMEs; · A Autoridade também participou do projeto cofinanciado pela CE e encerrado em janeiro de 2021, o *GDPR Compliance - Cloud Platform for Micro Enterprises*/ *SMOOTH*, em que foi desenvolvida uma plataforma na nuvem e um manual para microempresas para garantir o cumprimento do GDPR.

[83] EDPB (n. 58), p. 39; Smooth GDPR, **Smooth for Micro Enterprises**. Disponível em: <https://smoothplatform.eu/smooth-for-msmes/>. Acesso em 22 fev. 2021.

Lituânia[84]	· Participação de conferências, apresentações e seminários para PMES de diversos setores; · Publicação de material de orientação e FAQ; · Realização de reuniões com representantes de PMEs; · Consultas para PMEs; · PMEs é um dos públicos-alvo do projeto SolPriPa (cofinanciado pela CE) que tem como objetivo melhorar capacidade organizacional de entidades parceiras, promover conscientização sobre proteção de dados, promover engajamento de jovens, e melhorar a gestão de negócios para controladores e operadores.

[84] EDPB (n. 58), p. 40; State Data Protection Inspectorate, **Solving Privacy Box – SolPriPa project successfully implemented**. Disponível em: <https://vdai.lrv.lt/en/news/solpripa-project-successfully-implemented>. Acesso em: 22 fev. 2021.

Luxemburgo[85]	· Orientações às PMEs por e-mail e telefone; · Envio de *newsletter* mensal para 1700 assinantes; · Formulário simplificado e estruturado para notificações de incidentes de segurança; · Desenvolvimento de uma ferramenta de *self-assessment* de maturidade do GDPR (para empresas em geral), uma solução inovadora e intuitiva que permite aos usuários verificar o nível de *compliance* de suas organizações; · *Workshops* e criação do *Open Data Protection Laboratory* (DaProLab), um canal para troca de ideias em que o objetivo é ajudar os participantes a adotarem uma postura responsável (*accountability attitude)*; · Treinamento para empresários de PMEs e respectivas associações profissionais na identificação de seus stakeholders no contexto do GDPR; · Guia para empregadores e funcionários sobre vigilância no local de trabalho; · Participação em conferências e eventos voltados a novas empresas e empreendedores (startups)

[85] EDPB (n. 58), p. 40.

Malta[86]	· Desenvolvimento do projeto GDPRights, com duração de 24 meses e cofinanciado pela CE, para apoiar as PMEs no cumprimento do GDPR.
Polônia[87]	· Promoção de atividades de conscientização; · Elaboração de estudos temáticos no site, incluindo *guidelines* e manuais; · Cooperação com DPOs; · Linha direta para consulta e aconselhamento; · Envio de *newsletters* temáticas para mais de 6.000 assinantes.
Portugal[88]	· Desenvolvimento de dois modelos de registro de atividade de tratamento (para controladores e operadores);

[86] Ibid, p. 41; Office of the Information and Data Protection Commissioner, **GDPRights: GDPR awareness campaign and support to business organisations, in particular, SMEs**. Disponivel em: <https://idpc.org.mt/idpc-publications/gdpr-awareness-campaign-business-organisations-in-particular-smes/>. Acesso em: 22 fev. 2021.
[87] EDPB (n. 58), p. 42.
[88] Ibid.

	· Participação em várias iniciativas de sensibilização, a maioria destinadas a PMEs; · Orientação geral através de FAQ.
Reino Unido[89]	· Orientações e suporte específico para PMEs divulgados no site da ICO, incluindo: • FAQ para pequenas empresas; • Self-Assessment para proprietários de pequenas empresas e empresários individuais; • Diversos checklists para verificar *compliance*; • Modelo de aviso de privacidade; • Linha direta para consulta e aconselhamento às pequenas organizações; • Orientações e *checklist* para solicitações de acesso por titulares de dados; • Solicitação para visitas de aconselhamento *in-loco*.

[89] Apesar do *Brexit*, as iniciativas do Reino Unido foram consideradas. EDPB (n. 57), p. 44; Information Commissioner's Office, **Request for an advisory visit**. Disponível em: <https://ico.org.uk/global/request-for-an-advisory-visit>. Acesso em: 22 fev. 2021.

República Tcheca[90]	· Whitelist para operações de tratamento de dados pessoais isentas de DPIA; · Linha direta para consulta e aconselhamento;; · Organização de evento específico para PMEs que não precisam de DPO; · Apresentações sobre o GDPR e seminários, a maioria para PMEs.
Romênia[91]	· Participação em conferências, entrevistas e em reuniões de grupos de trabalho interinstitucionais; · Elaboração de materiais informativos e guias.
Suécia[92]	· Desenvolvimento de um guia interativo para PMEs para auxiliá-las no cumprimento do GDPR; · Participação em conferências, palestras e eventos destinados a PMEs;

[90] EDPB (n. 58), p. 44.
[91] Ibid, p. 43.
[92] Ibid, p. 44; Government Services for Business, **GDPR Guide**. Disponível em: <https://www.verksamt.se/web/international/running/the-gdpr-a-new-general-data-protection-regulation/the-gdpr-guide>. Acesso em: 22 fev. 2021.

	· Relatório nacional de privacidade que ilustrou os diferentes problemas para as PMEs cumprirem com as obrigações do GDPR; · FAQ, *guidelines* e outras publicações são feitas com linguagem fácil e compreensível, especialmente tendo em conta o titular dos dados e as PMEs.