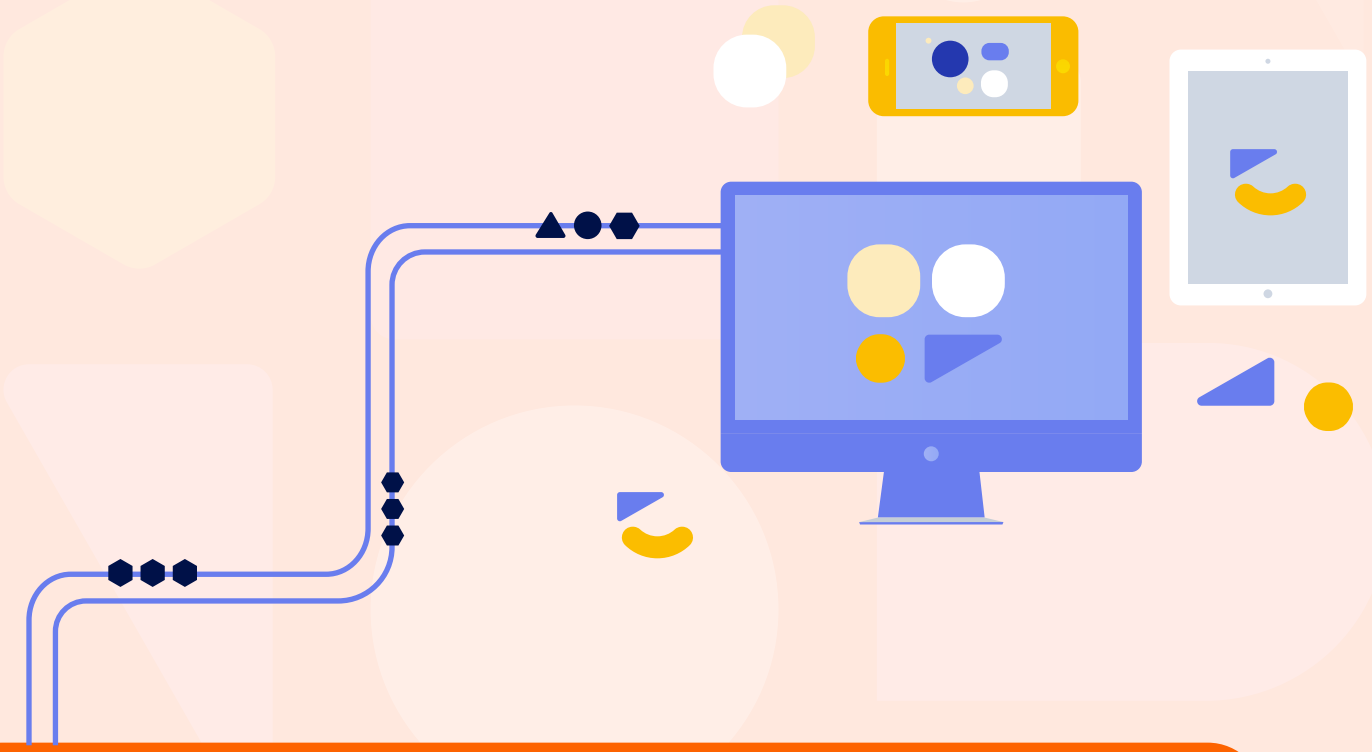


Design Apropriado para a Idade:

Código de Práticas para Serviços On-line

TRADUÇÃO
Beatriz Laus Marinho Nunes

REVISÃO
Carolina Braz Morena

Realização:

ITS

alana

Apoio:

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ÍNDICE

APRESENTAÇÃO DA TRADUÇÃO POR INSTITUTO DE TECNOLOGIA E SOCIEDADE

A Internet e as tecnologias de informação e comunicação são instrumentos muito poderosos e importantes para todos - inclusive para crianças e adolescentes. Segundo dados do UNICEF, antes da pandemia, as crianças já representavam um terço - dos usuários da internet.[3] Os benefícios da internet são muitos, mas você já parou para pensar que a internet por elas navegada e as estruturas das principais plataformas digitais são, em grande maioria, pensadas para o público adulto? Como todos nós que pertencemos à sociedade digitalmente conectada, crianças e adolescentes também têm seus dados coletados e muitas vezes utilizados para perfilamento e classificação de suas preferências e modos de vida.

No entanto, diferentemente de adultos as consequências da *data--driven* society não necessariamente estão claras para crianças e adolescentes. Isso é particularmente relevante tendo em vista que atravessam uma peculiar fase de desenvolvimento, na qual é natural - e muito relevante - ter um espaço livre de experimentações e inclusive cometer erros. Ainda mais para essa geração, uma das primeiras nascidas e criadas em um contexto de hiperdigitalização e datificação massiva.

É urgente e essencial discutir a sua proteção em ambientes digitais. Há aqui uma crescente necessidade de equilibrar a proteção dos dados e a privacidade de crianças e permitir o desenvolvimento em contato com o espaço digital que hoje é intrínseco à vivência de seus direitos.

A empreitada que se faz aqui é buscar adicionar um elemento nesse processo de buscar esse duplo objetivo de proteção da privacidade e promoção da liberdade de expressão e outros direitos. Busca-se aqui com a tradução do *Age-Appropriate Design Code* proposto pelo *Information Commissioner ‘s Office (ICO)* do Reino Unido propor um caminho, um exemplo de regulação a guiar a formulação de uma regulação específica para o Brasil.

Para contextualizar a importância e os objetivos desta tradução, cumpre fazer, em um primeiro momento, um breve mergulho no arcabouço jurídico de proteção aos direitos das crianças e adolescentes.

Esta parcela da população recebeu proteção especial pelos ordenamentos jurídicos brasileiro e internacional, consoante as conquistas do século XX. Neste período se reconheceu a necessidade de um olhar

3. The State of the World 's Children 2017 – Children in a digital world. Unicef, 2017. Disponível em https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf.

diferenciado para para crianças e adolescentes, em razão de suas características específicas, de estarem em processo de desenvolvimento e formação de sua personalidade. Avançamos desde a Declaração de Genebra sobre os Direitos das Crianças e Adolescentes até o recém publicado Comentário Geral nº 25 do Comitê das Nações Unidas sobre os Direitos das Crianças para entender as peculiaridades desse grupo e dar vazão a seus direitos humanos. Este último documento, já foca justamente no ambiente digital, detalha como a Convenção sobre os Direitos da Criança, um dos maiores marcos em prol dos dos direitos da criança e o tratado de direitos humanos mais aceito da história, se aplica igualmente ao mundo digital.

No Brasil, ao lado da supramencionada Convenção Internacional dos Direitos da Criança, ratificada pelo Brasil em 1990, já estava em vigor a Constituição de 1988, que assegurou, principalmente pela redação do Art. 227, a proteção a crianças e adolescentes como prioridade absoluta; atribui responsabilidade compartilhada entre Estado, família e sociedade; e dentre outros direitos, estabeleceu o direito à educação e à privacidade.

Nessa esteira, a década de 90 marca a consolidação dos direitos garantidos na Constituição. O Estatuto da Criança e do Adolescente (Lei 8.069 de 1990), um dos instrumentos legislativos mais avançados do mundo, condensou e direcionou toda a aplicação dos direitos fundamentais das pessoas menores de 18 anos no Brasil.[4] A lei reafirma essa prioridade absoluta e também a responsabilidade compartilhada entre Estado, família, e sociedade, bem como o direito de crianças e adolescentes à privacidade e à educação. O Estatuto destaca ainda que é direito das mães, pais ou responsáveis por crianças e adolescentes ter ciência de seu processo pedagógico e participar da definição das propostas educacionais. Além disso, determina que a criança e o adolescente têm direito a produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento - o que, no uso da internet, se conecta ao conceito de direitos da criança desde a concepção, no qual o desenvolvimento e a execução de serviços e produtos digitais utilizados por crianças devem atender verdadeiramente ao seu melhor interesse. Finalmente, tem-se o Código de Defesa do Consumidor (Lei 8.078 de 1990) que garante aos consumidores o direito à informação clara e adequada sobre os produtos e serviços que consome, protegendo-os contra práti-

4. "Em cumprimento ao comando constitucional, sobreveio a Lei 8.069/90 - reconhecida internacionalmente como um dos textos normativos mais avançados do mundo -, que adotou a doutrina da proteção integral e prioritária como vetor hermenêutico para aplicação de suas normas jurídicas, a qual, sabidamente, guarda relação com o princípio do melhor interesse da criança e do adolescente, que significa a opção por medidas que, concretamente, venham a preservar sua saúde mental, estrutura emocional e convívio social." (STJ, 4ª T., REsp 1587477/SC, Rel. Min. Luis Felipe Salomão, julg. 10/03/2020, DJe 27/08/2020)

cas abusivas - como aquelas que coloquem em risco a privacidade de crianças e adolescentes.

Na década seguinte temos a edição da norma que inaugura a proteção da privacidade dos usuários de Internet no Brasil, o Marco Civil da Internet (Lei 12.965 de 2014). Este marco legislativo modelo, concebido a partir de um processo de consulta multissetorial, estabeleceu como princípios para o uso da Internet no país a proteção à privacidade e aos dados pessoais (art. 3°, II e III), a preservação de segurança e funcionalidade da rede por técnicas compatíveis com padrões internacionais e estímulo ao uso de boas práticas (art. 3°, V), bem como determinou regras para a coleta dos dados, dentre elas a exigência do consentimento do titular para o uso e tratamento das informações (art. 7°, VII a X), dentre outros. Foi feita breve referência às crianças e adolescentes no art. 29 da lei, prevendo responsabilidade conjunta do poder público, sociedade civil, provedores de conexão e de aplicações de internet para promover sua educação e inclusão digital por meio de boas práticas.

Chegamos então a 2018, quando foi publicada a Lei Geral de Proteção de Dados (Lei 13.709 de 2018), detalhando sobre a proteção e o tratamento de dados pessoais, aí se incluindo, pela primeira vez, dispositivos de aplicação específica a crianças e adolescentes (art. 14). De fato, a LGPD reitera a preocupação da Constituição e do ECA com relação à busca do melhor interesse da criança e do adolescente como fundamento básico de toda e qualquer ação que visa a proteção desse público.[5]

Decerto que o zelo pelos dados de crianças e adolescentes não deve ser imposto somente ao núcleo familiar, pois ele deve competir, em primeiro lugar, ao próprio Poder Público e às empresas privadas que realizam coleta e tratamento de dados, agentes hiper suficientes nessa relação. Afinal, a busca pelo atendimento ao melhor interesse da criança e do adolescente também compete ao Estado e à sociedade.

Todavia, no Brasil, ainda que exista um arcabouço protetivo de crianças e adolescentes robusto, necessitando de diretrizes específicas sobre os instrumentos a serem empregados para garantir a consolidação e a efetividade dos direitos previstos em lei no ambiente digital. Desenvolvedores e fornecedores que trabalham no ambiente digital podem atuar melhor tendo balizas claras para seu funcionamento, para gerar maior proteção e segurança jurídica.

Existe aí uma necessidade e também uma oportunidade para a nossa Autoridade Nacional de Proteção de Dados, que na sua agenda regulatória para o biênio 2021-2022 não contemplou infelizmente a regu-

---

5. "(...) o princípio do melhor interesse da criança e do adolescente prescrito no art. 227 da Constituição Federal, no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e na Convenção sobre os Direitos da Criança, incorporada ao ordenamento pátrio pelo Decreto nº 99.710/1990, consagra que, a partir do caso concreto, os aplicadores do direito devem buscar a solução que proporcione o maior benefício possível para a criança, vulnerável por natureza. Portanto, é de extrema importância garantir a efetividade aos direitos fundamentais da criança e do adolescente (...)." (STJ, REsp 1713123 / MS, 3ª T., Rel. Min. Ricardo Vilas Boas Cueva, julg. 6.3.2018, DJ 12.3.2018).

lamentação da proteção de dados infantis.

Vale lembrar que o recém editado Comentário nº 25 sobre os Direitos das Crianças em Ambiente Digital do Comitê dos Direitos das Crianças das Nações Unidas destaca a necessidade de se estabelecer diretrizes de boas práticas. Essa é uma obrigação reconhecida ao Poder Público brasileiro no art. 29, parágrafo único, do Marco Civil da Internet e recomendada aos controladores e operadores nos artigos 50 e 51 da Lei Geral de Proteção de Dados.

Além da necessidade de guias claros de aplicação da Lei Geral no que tange a proteção dos dados pessoais de crianças e adolescentes existe aí também uma oportunidade de protagonismo regional para a nossa Autoridade. Outros países da América Latina já possuem legislação sobre a proteção de dados de crianças e adolescentes – como a Colômbia, por exemplo, mas ainda nenhuma autoridade editou um documento de recomendação de boas práticas nesse sentido com foco no *design* de ferramentas que contemple os direitos das crianças.

É diante deste cenário que o Instituto de Tecnologia e Sociedade, com fundamental apoio do Ministério de Relações Exteriores e Desenvolvimento do Reino Unido, e em parceria com o Instituto Alana, desenvolveu o projeto Proteção de Crianças e Adolescentes em Ambientes Digitais. Esta iniciativa faz parte do projeto conjunto intitulado “Fostering a Stronger Data Protection Framework in Brazil” (“Promovendo uma estrutura de proteção de dados pessoais mais forte no Brasil”, em português).

Diversos países têm instituído orientações para empresas e desenvolvedores de serviços *online* para a adoção de boas práticas, no sentido de estruturar uma governança na internet no sentido de contribuir para o desenvolvimento infantojuvenil, reduzindo os riscos e protegendo os dados. O Reino Unido seguiu o caminho da regulação harmonizando proteção de dados e proteção de direitos das crianças e adolescentes. A *Information Commissioner’s Office*, autoridade de proteção de dados, editou, em setembro de 2020, o presente Código de Práticas para os Serviços *Online*. O documento visa a orientar que serviços digitais sejam apropriados para a idade de crianças e adolescentes e protejam adequadamente seus direitos. Trata-se de regulação adotada pela autoridade (ICO) para especificar a lei de proteção de dados e a compatibilizar com os diferentes direitos de crianças e adolescentes.[6] Essa regulação - em formato de código - obriga prestadores a se adequarem após um período de um ano. O código é bastante compreensivo e conta com exemplos claros para garantir a adequação dos provedores de serviços às suas

6. O código segue as bases e referências tanto do Data Protection Act – Lei de Proteção de Dados no âmbito do Reino Unido) quanto da General Data Protection Regulation - Lei Geral de Proteção de Dados da União Europeia

diretrizes e às normas existentes.

Assim, esperamos que esta tradução possa auxiliar a informar o debate no Brasil para orientar práticas que resguardem a privacidade e demais direitos fundamentais no ambiente digital especificamente no caso desses sujeitos, atendendo seu melhor interesse. Além disso, diante da proximidade da plena vigência da LGPD, é mais do que necessário que os direitos nela previstos alcancem a efetividade, o que só será plenamente possível por meio de uma regulação clara, que oferte balizas de condutas e práticas principalmente aos desenvolvedores de aplicações e fornecedores de serviços digitais.

É essencial que sejam desenvolvidas formas para que a Internet ofereça todo seu potencial de aprendizado e interação para a população infantojuvenil de um modo que seja coerente com o sistema protetivo e que permita o desenvolvimento livre das crianças e adolescentes. Este serve como uma indicação para o início de um debate público para auxiliar no processo da Autoridade Nacional de Proteção de Dados de estabelecer diretrizes para a proteção de crianças e adolescentes.

APRESENTAÇÃO DA TRADUÇÃO POR INSTITUTO ALANA

A presença de crianças na internet em idade cada vez mais tenra coloca-se, hoje, como uma realidade irreversível e incontornável. Dados da pesquisa TIC Kids Brasil 2019 [7] apontam que, no Brasil, 91% das pessoas de 9 a 17 anos acessam a Internet pelo menos uma vez por dia, sendo que 42% das crianças começam a fazê-lo antes dos oito anos de idade. A crescente utilização de mídias digitais pelo público infantil, contudo, levanta sérias preocupações a respeito da garantia dos direitos desses indivíduos no ambiente on-line, especialmente no que toca à tutela de sua privacidade e proteção de seus dados pessoais.

À medida em que crianças passam a utilizar a internet com maior intensidade, passam a se expor, de maneira igualmente intensa, à coleta massiva de seus dados pessoais, os quais são objeto de inúmeras operações de tratamento pelas empresas que atuam nesse ecossistema visando a finalidades diversas – muitas das quais incompatíveis com o melhor interesse desses indivíduos, que, em razão do não desenvolvimento pleno de suas capacidades de discernimento, tornam-se particularmente vulneráveis aos malefícios que podem advir do uso inadequado e desleal de seus dados.

Por isso, a necessidade de adoção de medidas especiais de proteção às crianças na internet vem sendo reconhecida ao redor de todo o mundo. Recentemente, o Comitê dos Direitos da Criança da ONU publicou o seu Comentário Geral nº 25, que trata justamente das medidas que devem ser implementadas, sobretudo pelos Estados, para garantir uma experiência digital segura às crianças.

A garantia dos direitos das crianças no ambiente digital é, contudo, dever que cabe não somente ao Estado, na formulação de políticas públicas; tampouco somente às famílias, na orientação e estabelecimento de limites a seus pequenos. Cabe, isso sim, a esses dois atores em conjunto, bem como a toda a sociedade civil e, especificamente, às empresas que a compõem e oferecem serviços digitais utilizados massivamente por crianças. É essa a orientação consubstanciada no artigo 227 de nossa Constituição Federal, que, de maneira inovadora, estabelece a responsabilidade transversal e compartilhada na garantia dos direitos das crianças com absoluta prioridade.

É a partir dessa ótica de responsabilização compartilhada que deve ser lido o presente código de *design*, desenvolvido pela *Information*

7. [1] CETIC.BR – Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. TIC KIDS ONLINE BRASIL. 2019. Disponível em <https://cetic.br/pt/pesquisa/kids-online/>. Acesso em 16.07.2021.

Commissioner's Office (ICO – agência regulatória britânica) visando justamente a endereçar as preocupações aqui tangenciadas. Nele, localizam-se 15 padrões com vistas a orientar as empresas cujos serviços on-line são utilizados por crianças quanto ao modo de garantir que estejam oferecendo uma experiência digital segura e respeitosa à privacidade desses indivíduos. Padrões dessa natureza podem, e devem, ser levados em conta pelas empresas que atuam no Brasil, cuja corresponsabilidade pela garantia dos direitos digitais das crianças, como se viu, está posta constitucionalmente.

Os padrões descritos neste código compreendem desde princípios a serem observados no *design* e oferecimento dos produtos – como a transparência e o melhor interesse das crianças – até a limitação a determinadas práticas potencialmente danosas aos pequenos, como o perfilamento e a utilização de técnicas de *nudge*. Trata-se, portanto, de conjunto de orientações bastante diverso, que fornece desde diretrizes de caráter abrangente e principiológico até regras relativas a produtos e práticas comerciais específicas.

O código vem, ainda, acompanhado de anexos úteis à adequada implementação dos padrões ali descritos. São fornecidos: (i) um diagrama que visa a auxiliar as empresas a compreender se seus serviços devem cumprir com as disposições do código; (ii) considerações gerais sobre o desenvolvimento progressivo das capacidades das crianças e as peculiaridades de cada faixa etária; (iii) considerações gerais sobre as bases legais para o tratamento de dados; e (iv) modelo de relatório de impacto à proteção de dados pessoais, cuja confecção está dentre os padrões a serem observados pelas empresas que promovem o tratamento dos dados de crianças.

Cabem, por fim, duas considerações preliminares que devem permear a leitura de todo o código pelo público brasileiro.

Em primeiro lugar, ainda que o texto tenha sido, evidentemente, pensado a partir do regime do GDPR (General Data Protection Regulation) europeu, as suas disposições não são desarmônicas com a LGPD (Lei Geral de Proteção de Dados Pessoais) brasileira, mesmo porque o texto pátrio foi em grande parte inspirado na normativa europeia, especialmente no que diz respeito aos princípios gerais que regem a tutela dos dados pessoais. A 'lealdade' (fairness), por exemplo, tão mencionada ao longo do texto, ecoa em larga medida o nosso instituto da boa-fé objetiva, que deve permear todas as atividades de tratamento de dados (art. 6º da LGPD) e servir como cláusula geral nas relações entre particulares.

Depois, é importante que se tenha em mente que as crianças a que se refere o código devem ser lidas, por nós, como 'crianças e adolescentes'. Isso porque o código adotou a definição de criança da Convenção dos Direitos da Criança da UNICEF, que considera como criança "todo ser humano com menos de 18 anos de idade". O Estatuto da Criança e do Adolescente brasileiro, por outro lado, define criança como "a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade" (art. 2º do ECA). Importante que se tenha em mente, portanto, que os adolescentes não estão à margem das salvaguardas previstas neste código.

Espera-se, assim, que este documento auxilie as empresas que atuam no Brasil na adoção de boas práticas voltadas à infância. Espera-se, ainda, que possa inspirar os órgãos regulatórios competentes e os diversos atores da sociedade civil organizada a se debruçar sobre os temas da infância no mundo digital de maneira prática, propositiva e orientada à implementação de medidas que garantam, efetivamente, uma experiência on-line segura e respeitosa aos direitos das crianças, e, por consequência, aos direitos de todos nós.

PREFÁCIO DA AUTORIDADE DE PROTEÇÃO DE DADOS DO REINO UNIDO *(ICO - INFORMATION COMMISSIONER)*

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

O Secretário de Estado do Reino Unido atribuiu o *Design* Apropriado para a Idade ao Parlamento, em cumprimento à seção 125(1)(b), da Lei de Proteção de Dados de 2018 (DPA 2018)[1], em 11 de junho de 2020. A Autoridade de Proteção de Dados do Reino Unido (ICO)[2] publicou o código em 12 de agosto de 2020, e entrará em vigor em 2 de setembro de 2020, com 12 meses de período para transição.

Há mais informações no Memorando Explanatório.

Prefácio da Autoridade de Proteção de Dados do Reino Unido *(ICO - Information Commissioner)*

Dados encontram-se hoje no âmago dos serviços digitais que crianças usam diariamente. A partir do momento em que um jovem abre um aplicativo, joga um jogo ou carrega um site, dados começam a ser coletados. Quem está usando o serviço? Como eles estão utilizando o serviço? Com que frequência? De onde? Em que dispositivo?

Essas informações podem então informar técnicas usadas para persuadir crianças e adolescentes a passarem mais tempo utilizando serviços, moldar o conteúdo com os quais são encorajados a se engajar e personalizar os anúncios que aparecem para eles.

Considerando todos os benefícios que a economia digital pode oferecer às crianças, atualmente não estamos criando um espaço seguro para que elas aprendam, explorem e brinquem.

Este código de conduta de práticas visa a mudar isso, não ao proteger as crianças do mundo digital, mas ao protegê-las dentro dele.

Este código é necessário.

Este código levará a mudanças que ajudarão a empoderar tanto adultos quanto crianças.

Um em cada cinco usuários de internet no Reino Unido são crianças, mas elas estão usando uma internet cujo *design* não foi feito para elas.

---

1. *Data Protection Act 2018 (The Act)*: A Lei de Proteção de Dados de 2018 é a implementação pelo Reino Unido do Regulamento Geral de Proteção de Dados (GDPR). Disponível em: <https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018,organisations%2C%20businesses%20or%20the%20government.&text=Everyone%20responsible%2-0for%20using%20personal,used%20fairly%2C%20lawfully%20and%20transparently>. Acesso em: 21 de maio, 2020.

2. *Information Commissioner's Office (ICO)*. Acessar: <https://ico.org.uk/>.

Em nossa própria pesquisa, realizada a fim de fundamentar o código, ouvimos crianças descrevendo práticas referentes a pesquisa e coleta de dados como “intrometidas”, “rudes” e “um pouco esquisitas”.

Nossa recente pesquisa nacional sobre as principais preocupações das pessoas com relação à proteção de dados classificou a privacidade das crianças em segundo lugar, apenas atrás da segurança cibernética. Isso reflete conclusões semelhantes em pesquisas realizadas pelo Escritório de Comunicações do Reino Unido (Ofcom) e pela Escola de Economia e Ciência Política de Londres (LSE).

Este código levará a mudanças nas práticas que outros países também vêm considerando.

Ele está enraizado na Convenção das Nações Unidas sobre os Direitos da Criança (CNUDC), a qual reconhece as salvaguardas especiais que as crianças precisam em todos os aspectos de suas vidas. A lei de proteção de dados no âmbito europeu reflete esse reconhecimento e fornece suas próprias proteções adicionais para as crianças.

Apesar de o código ser considerado como um dos pioneiros no que tange ao assunto abordado, ele reflete a direção global das reformas sendo consideradas pelos EUA, pela Europa e, globalmente, pela Organização para Cooperação e Desenvolvimento Econômico (OCDE).

Este código levará a mudanças almejadas pelo Parlamento do Reino Unido.

O Parlamento e o governo asseguraram que as leis de proteção de dados do Reino Unido, verdadeiramente, transformarão a forma com que protegem crianças on-line, ao exigir que a ICO introduzisse este código de práticas para serviços on-line.

O código cumpre esse mandato e exige que os serviços da sociedade de informação coloquem o melhor interesse da criança em primeiro lugar, quando projetarem e desenvolverem aplicativos, jogos, brinquedos conectados e sites que serão de provável acesso por crianças.

Este código é alcançável.

O código não é uma nova lei, mas estabelece parâmetros e explica como o Regulamento Geral sobre a Proteção de Dados (RGPD) se aplica ao contexto de crianças usuárias de serviços digitais. Ele seguiu um processo completo de consulta, que incluiu conversas com pais, crianças, escolas, grupos de campanha infantil, desenvolvedores, empresas de tecnologia e jogos e provedores de serviços on-line.

Essas conversas ajudaram a moldar nosso código em provisões eficazes, proporcionais e alcançáveis.

As organizações devem se adequar ao código e comprovar que seus serviços utilizam dados de crianças de forma justa e em conformidade com a lei de proteção de dados.

O código é um conjunto de 15 parâmetros flexíveis – eles não proíbem ou especificamente prescrevem – que fornecem uma proteção integrada, a fim de permitir que as crianças explorem, aprendam e brinquem on-line, assegurando que o melhor interesse da criança seja a principal consideração ao fazer o *design* de serviços e desenvolvê-los on-line.

As configurações devem ser, por definição, de "alta privacidade" (a menos que haja um motivo imperioso para não o fazer); apenas a quantidade mínima de dados pessoais deve ser coletada e retida; os dados das crianças não devem, via de regra, ser compartilhados; os serviços de geolocalização devem ser desativados por padrão. Técnicas de *Nudge* não devem ser usadas para encorajar as crianças a fornecer dados pessoais desnecessários, enfraquecer ou desativar suas configurações de privacidade. O código também aborda questões de controle parental e perfilamento.

Este código fará a diferença.

Os desenvolvedores e aqueles do setor digital devem agir. Permitimos o período máximo de transição de 12 meses e continuaremos trabalhando com a indústria.

Queremos que os codificadores, os *designers* UX e os engenheiros de sistemas se comprometam a cumprir com estes parâmetros em seu dia a dia de trabalho e estamos criando um pacote de apoio para ajudar.

O próximo passo deve ser um período de ação e preparação. Acredito que as empresas desejarão estar em conformidade com os parâmetros, pois vão querer demonstrar seu compromisso em agir sempre no melhor interesse da criança. As empresas que não fizerem as mudanças necessárias correm o risco de sofrer ações regulatórias.

Além disso, elas [as empresas] correm o risco de ser ultrapassadas por aquelas organizações que estejam dispostas a se adequar.

Na próxima geração, acredito que olharemos para trás e acharemos peculiar que os serviços on-line nem sempre tenham sido projetados com as crianças em mente.

Quando meus netos estiverem crescidos e tiverem filhos, a necessidade de manter as crianças seguras on-line será tão importante quanto a necessidade de assegurar que elas comam de forma saudável, recebam

uma boa educação ou usem o cinto de segurança, mesmo que no banco de trás de um carro.

E, embora nosso código nunca substitua o controle parental e a orientação dos pais, ele ajudará as pessoas a terem mais confiança de que seus filhos possam aprender, explorar e brincar on-line com segurança.

Não há dúvida de que uma mudança é necessária. O código é uma parte importante e significativa dessa mudança.

Elizabeth Denham CBE

RESUMO EXECUTIVO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

As crianças são cada vez mais "datificadas" à medida que crescem, com empresas e organizações registrando milhares de dados sobre eles. Os dados podem variar, desde detalhes sobre seu estado de espírito e suas amizades, até a hora em que acordaram e quando foram dormir.

A conformidade com este código de práticas garantirá que você, enquanto organização prestadora de serviços on-line com probabilidade de ser acessada por crianças no Reino Unido, estará levando em conta o melhor interesse da criança. Este código ajudará no desenvolvimento de serviços que reconheçam e atendam ao fato de que as crianças merecem proteção especial na forma como seus dados pessoais são utilizados, ao mesmo tempo que ofereçam oportunidades para as crianças explorarem e se desenvolverem on-line.

Você tem 12 meses para implementar as mudanças necessárias, a partir da data em que o código entra em vigor, após o processo de aprovação parlamentar. A abordagem de *enforcement* da ICO estabelecida em nossa Política de Ação Regulatória se aplica para o cumprimento deste código. Tanto essa política, quanto este código aplicam uma abordagem proporcional e baseada em riscos.

A Convenção das Nações Unidas sobre os Direitos da Criança (CNUDC) reconhece que as crianças necessitam de proteção e de cuidados especiais em todos os aspectos de suas vidas. Constata-se que, tanto de forma internacional, como também dentro do Reino Unido, esforços ainda são necessários para a criação de um espaço on-line seguro, a fim de que as crianças possam aprender, explorar e brincar.

No Reino Unido, o Parlamento e o governo agiram para assegurar que nossas leis internas de proteção de dados realmente transformem a forma como protegemos nossas crianças quando elas acessam os serviços on-line, ao exigir que a ICO produzisse este código de práticas. Este código procura proteger as crianças dentro do mundo digital, ao invés de apenas impedir que o acessem.

O código estabelece 15 parâmetros de *design* adequados à idade, refletindo uma abordagem baseada em riscos. O objetivo é fornecer configurações padrão as quais assegurem que as crianças tenham o melhor acesso possível aos serviços on-line, minimizando a coleta e o uso de dados.

[O código] também assegura que **crianças as quais optam** por alterar suas configurações padrão recebam as informações, as orientações e os conselhos corretos, antes de fazê-lo, bem como proteção adequada relativa a como seus dados serão usados posteriormente.

Você deve seguir os parâmetros como parte de sua abordagem para cumprir com a lei de proteção de dados. Se puder nos mostrar que está em conformidade com esses parâmetros, estará também em conformidade com o código. Os parâmetros são cumulativos e interligados, e você deve implementar todos eles, na medida em que sejam relevantes ao seu serviço, a fim de demonstrar sua conformidade.

Os detalhes fornecidos abaixo dos parâmetros fornecem explicações adicionais para auxiliar na sua compreensão e na implementação deles na prática. Foram concebidos para ajudá-lo se você não tiver certeza do que fazer, mas não são taxativos. Isso deverá lhe trazer flexibilidade para desenvolver serviços que estejam de acordo com os parâmetros à sua própria maneira, adotando uma abordagem proporcional e baseada em riscos. Isso o ajudará a desenvolver serviços que estejam em conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e o Regulamento de Privacidade e Comunicações Eletrônicas (RPCE).

RECURSOS ADICIONAIS

Código de *Design* Apropriado para a Idade

PARÂMETROS DESTE CÓDIGO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Os parâmetros são:

1. **O melhor interesse da criança:** O melhor interesse da criança deve ser uma consideração primordial para o *design* e o desenvolvimento on-line de serviços de provável acesso por crianças.

2. **Relatório de impacto à proteção de dados pessoais:** Realizar um RIPD para avaliar e mitigar os riscos aos direitos e às liberdades das crianças que terão acesso ao serviço, que resultam do tratamento de dados. Considerar as diferentes idades, capacidades de desenvolvimento e assegurar que o seu RIPD esteja em conformidade com este código.

3. **Aplicação adequada à idade:** Adotar uma abordagem baseada em riscos para reconhecer a idade de usuários individuais e assegurar que você aplique efetivamente os parâmetros deste código a usuários infantis. Também estabelecer a idade com um nível de certeza adequado aos riscos inerentes a direitos e liberdades das crianças que surgem do tratamento de dados, ou aplicar os parâmetros deste código a todos os seus usuários.

4. **Transparência:** Todas as informações de privacidade que são fornecidas aos usuários, assim como demais termos, políticas e parâmetros publicados, devem ser concisas, destacadas e fornecidas em linguagem clara e adequada à idade da criança. Devem ser fornecidas explicações adicionais específicas, chamadas de "*bite-size*", isto é, de fácil compreensão, sobre como os dados pessoais são utilizados a partir do momento em que o uso do serviço ou da plataforma em questão é iniciado.

5. **Uso de dados de forma nociva:** Não utilizar os dados pessoais de crianças de formas que já foram provadas como nocivas ao seu bem-estar, ou que vão contra códigos de prática da indústria, outras disposições regulamentares ou orientações do governo.

6. **Políticas e padrões da comunidade:** Respeitar seus próprios termos, políticas e padrões da comunidade publicados (inclusive – mas não se limitando a – políticas de privacidade, restrição de idade, regras de comportamento e políticas de conteúdo).

7. **Configurações padrão:** As configurações devem ser 'alta privacidade' por padrão (a menos que você possa demonstrar uma razão convincente para uma configuração padrão diferente, levando em conta o melhor interesse da criança).

8. **Minimização de dados:** O mínimo de dados pessoais deve ser coletado e retido para que sejam fornecidos os elementos de seu serviço nos quais uma criança está ativa e conscientemente envolvida. Dar às crianças escolhas separadas sobre os elementos que elas desejam ativar.

9. **Compartilhamento de dados:** Não divulgar os dados das crianças, a menos que você possa demonstrar uma razão convincente para fazê-lo, levando em conta o melhor interesse da criança.

10. **Geolocalização:** Desativar as opções de geolocalização por padrão (a menos que você possa demonstrar uma razão convincente para que a geolocalização esteja ativada por padrão, levando em conta o melhor interesse da criança). Providenciar um aviso óbvio para crianças, quando o rastreamento de localização estiver ativo. As opções que tornam a localização de uma criança visível para terceiros devem ser desativadas, por padrão, ao final de cada sessão.

11. **Controles parentais:** Se você disponibilizar controles parentais, informe à criança, de maneira apropriada à sua idade, acerca desta funcionalidade. Se seu serviço on-line permitir que um pai/mãe ou responsável monitore a atividade on-line de seu filho/filha ou o local onde este se encontra, providenciar um aviso óbvio para a criança, quando ela estiver sendo monitorada.

12. **Perfilamento:** Desativar por padrão opções que utilizem o perfilamento (a menos que você possa demonstrar uma razão convincente para que o perfilamento esteja ativado por padrão, levando em conta o melhor interesse da criança). Só permitir o perfilamento se você tiver medidas apropriadas para proteger a criança de quaisquer efeitos nocivos (em particular, ser exposta a conteúdo prejudicial à sua saúde ou ao seu bem-estar).

13. **Técnicas de encorajamento *(nudge techniques)*[8]:** Não usar técnicas de encorajamento para conduzir ou encorajar crianças a fornecer dados pessoais desnecessários ou enfraquecer ou desativar suas proteções de privacidade.

---

8. NT. Também conhecido como a "Teoria do incentivo" no Brasil, o termo *nudge*, em português significa "empurrão". Esse conceito faz parte da economia comportamental, gênero da economia que busca oferecer melhores técnicas de persuasão através da união entre economia e psicologia. Disponível em: <https://startupi.com.br/2020/08/voce-sabe-o-que-significa-o-termo-*nudge*-no-mundo-dos-negocios/>. Acesso em 18 de maio de 2021.

14. **Brinquedos e dispositivos conectados:** Se você disponibilizar um brinquedo ou um dispositivo conectado, certifique-se de incluir ferramentas eficazes para permitir a conformidade com este código.

15. **Ferramentas on-line:** Disponibilizar ferramentas proeminentes e acessíveis para ajudar as crianças a exercer seus direitos de proteção de dados e relatar preocupações.

SOBRE ESTE CÓDIGO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

De forma resumida

Este código explica como assegurar que seus serviços on-line protejam adequadamente os dados pessoais de crianças. Você deve seguir o código para ajudá-lo a tratar os dados de crianças de forma justa. Ele também permitirá que você desenvolva serviços que cumpram, e demonstrem que você cumpre, com o RGPD e os Regulamentos de Privacidade e Comunicações Eletrônicas (RPCE). Se você não cumprir com este código, provavelmente terá mais dificuldades para demonstrar sua adequação à lei, caso tomemos medidas regulatórias contra você.

- A quem se destina este código?
- Qual é o propósito deste código?
- Qual é o status deste código?
- Como devemos usar o código?

A quem se destina este código?

Este código é destinado a prestadores de serviços da sociedade de informação (SSI). Aplica-se a você, se você fornece produtos ou serviços on-line (incluindo aplicativos, programas, sites, jogos ou ambientes comunitários, e brinquedos ou dispositivos conectados com ou sem uma tela) que processam dados pessoais e são de provável acesso por crianças no Reino Unido. Não é apenas para serviços destinados a crianças. Neste código, “serviço on-line” implica um SSI relevante. Para mais informações, veja a seção sobre serviços abrangidos por este código.

Qual é o propósito deste código?

Este código aborda como desenvolver salvaguardas de proteção de dados em serviços on-line para assegurar que estes sejam apropriados para uso por crianças, e satisfaçam suas necessidades de desenvolvimento.

O código reflete a crescente preocupação com a situação em que se encontram as crianças no contexto da sociedade atual e do mundo digital moderno. Internacionalmente, e assim como no Reino Unido, há um entendimento geral de que mais esforços devem ser feitos para o

desenvolvimento de um espaço on-line seguro no qual crianças possam aprender, explorar e brincar. Este código consegue atingir esse propósito, não ao protegê-las contra o mundo digital, mas sim dentro dele.

A CNUDC reconhece que as crianças precisam de salvaguardas e cuidados especiais em todos os aspectos de suas vidas e exige que esses sejam assegurados por proteções legais apropriadas. A lei de proteção de dados no âmbito europeu reflete esse reconhecimento e fornece suas próprias proteções adicionais para as crianças.

No Reino Unido, o Parlamento e o governo agiram para assegurar que nossas leis internas de proteção de dados transformassem, verdadeiramente, a forma como protegemos as crianças, quando elas acessam os serviços on-line, exigindo da Autoridade a elaboração deste código de práticas. Este código é uma consequência da intenção do Parlamento e do governo de usar a lei de proteção de dados para fazer uma mudança profunda e duradoura na forma como cuidamos de crianças quando elas acessam serviços on-line.

Ele leva em conta os padrões e os princípios estabelecidos na CNUDC e estabelece proteções específicas para os dados pessoais de crianças, em conformidade com as disposições do RGPD.

Se você fornecer serviços relevantes on-line, este código o ajudará a cumprir e a demonstrar que você cumpre com suas obrigações de proteção de dados. A conformidade com os parâmetros deste código será uma medida fundamental para o cumprimento das leis de proteção de dados. Adequar-se a este código também mostrará aos pais e a outros usuários de seus serviços que você compreende a seriedade da proteção de dados pessoais de crianças, fazendo transparecer a sua confiabilidade e demonstrando que seus serviços são adequados para que as crianças os utilizem.

Como este código considera os direitos da criança?

Ao preparar este código, a Autoridade [ICO] é obrigada a considerar as obrigações do Reino Unido submetidas à CNUDC e o fato de que as crianças têm necessidades a depender da idade.

O código incorpora o princípio-chave da CNUDC de que o melhor interesse da criança deve ser uma preocupação primordial em todas as ações relativas às crianças. Ele também visa a respeitar os direitos e os deveres dos pais e a capacidade progressiva da criança de fazer suas próprias escolhas.

Este código visa a garantir que os serviços on-line utilizem os dados pessoais de crianças de forma a apoiar os direitos da criança no que diz respeito a:

- liberdade de expressão;
- liberdade de pensamento, consciência e religião;
- liberdade de associação;
- privacidade;
- acesso a informações da mídia (mas com proteção adequada, para evitar acesso a informações e materiais prejudiciais ao seu bem-estar);
- brincar e se envolver em atividades recreativas apropriadas à sua idade; e
- proteção contra exploração econômica, sexual ou qualquer outra forma de exploração.

Como este código auxilia os pais?

Os pais (ou os responsáveis legais) desempenham um papel fundamental na proteção de seus filhos e na decisão do que é de seu melhor interesse. Entretanto, no contexto dos serviços on-line, pais e filhos podem achar difícil fazer escolhas informadas ou exercer qualquer controle sobre a forma como esses serviços utilizam os dados das crianças. Muitas vezes, a única escolha, na prática, é evitar completamente os serviços on-line, o que significa que a criança perde os benefícios de brincadeiras, interação e desenvolvimento on-line. Este código espera, portanto, que os provedores desses serviços assumam a responsabilidade de assegurar que a forma com que os seus serviços utilizam dados pessoais seja adequada à idade da criança, leve em conta seu melhor interesse e respeite seus direitos; além de apoiar os pais ou as crianças mais velhas a fazer escolhas (quando for apropriado) no melhor interesse da criança.

Como este código incentiva a obrigação de cumprimento da proteção de dados?

O regime de proteção de dados do Reino Unido está estabelecido na Lei de Proteção de Dados de 2018 (DPA 2018) e no Regulamento Geral sobre a Proteção de Dados (RGPD). Esse regime exige que você adote uma abordagem baseada em riscos quando utiliza os dados das pessoas, com base em princípios-chave, direitos e obrigações.

Este código apoia a conformidade com esses princípios gerais ao elencar proteções específicas, que devem ser inseridas, ao desenvolver serviços on-line prováveis de serem acessados por crianças, de acordo com o Considerando 38 do RGPD:

> "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das salvaguardas em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, notadamente, à utilização de dados pessoais de crianças para efeitos de marketing ou para criação de perfis ou de usuários, além de ser aplicada também quanto ao tratamento de dados pessoais em relação às crianças, ao utilizarem serviços oferecidos diretamente a uma criança..."

Este código estabelece medidas práticas e salvaguardas para assegurar que o tratamento submetido ao RGPD possa ser considerado 'leal' no contexto de riscos on-line para crianças e o ajudará a cumprir com as seguintes obrigações:

- Artigo 5(1)(a): princípio da licitude, lealdade e transparência[9];
- Artigo 5(1)(b): princípio da finalidade do tratamento;
- Artigo 5(1)(c): princípio da minimização de dados;
- Artigo 5(1)(d): princípio da limitação de armazenamento;
- Artigo 5(2): princípio da prestação de contas;
- Artigo 6: licitude do tratamento;
- Artigos 12, 13 e 14: direito à informação;
- Artigos 15 a 20: direitos do titular de dados;
- Artigo 22: perfilamento e decisões automatizadas;
- Artigo 25: proteção de dados desde a concepção e por padrão (*data protection by design and by default*);
- Artigo 35: relatório de impacto à proteção de dados pessoais (RIPD).

O código abrange o uso de 'dados inferidos' (informações sobre uma criança que você não coleta diretamente, mas que você deduz de outras informações ou de seus comportamentos on-line), bem como dados que você coleta diretamente da criança.

O Anexo C também inclui algumas orientações sobre como identificar sua base legal para tratamento de dados, no contexto de um

9. No original: Article 5 GDPR. Principles relating to processing of personal data. 1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). Os dados pessoais do usuário serão tratados de forma lícita, leal e transparente (licitude, lealdade e transparência).

serviço on-line. Se você se basear no consentimento, ele explica a regra do Artigo 8, sobre consentimento parental em relação a crianças menores de 13 anos.

Os Regulamentos de Privacidade e Comunicações Eletrônicas (RPCE) também estabelecem algumas regras específicas sobre o uso de *cookies* e outras tecnologias que dependem do acesso aos dispositivos do usuário e de mensagens de marketing eletrônico. Este código se refere a essas exigências quando forem relevantes, contudo, para obter mais detalhes sobre como cumprir com essas exigências, você também deve ler nosso Guia RPCE à parte.

Se você precisar tratar dados pessoais a fim de proteger as crianças de danos on-line, como, por exemplo, impedir qualquer forma de exploração e de abuso sexual infantil, então este código não deve impedir que você assim o faça. Entretanto, você precisa cumprir todas as exigências padrão de proteção de dados antes de prosseguir, como assegurar que o tratamento seja justo e proporcional aos danos que você está procurando evitar, identificar uma base legal para o tratamento e disponibilizar informações transparentes.

Qual é o status legal deste código?

Este é um código de práticas elaborado nos termos da seção 123, da DPA 2018:

> "A Comissão deve preparar um código de práticas que contenha as orientações que considerar apropriadas sobre os padrões de *design* adequados à idade, em relação aos serviços relevantes da sociedade de informação que serão de provável acesso por crianças."

Foi apresentado ao Parlamento em 11 de junho de 2020, e publicado em 12 de agosto de 2020, sob a seção 125, da DPA 2018. Entra em vigor em 2 de setembro de 2020.

Conforme esclarecido nos debates Parlamentares, quando o Projeto de Lei de Proteção de Dados foi aprovado pelo Parlamento, se o seu serviço on-line não cumprir com uma das disposições deste código, será mais difícil demonstrar a sua conformidade com a lei e você poderá sofrer ações regulatórias.

De acordo com a seção 127 da DPA 2018, a Autoridade deve considerar o código ao analisar se um serviço on-line cumpriu com suas obrigações de proteção de dados nos termos do RGPD ou do RPCE. Em especial, a Autoridade levará o código em consideração ao avaliar questões de licitude, lealdade, transparência e responsabilidade sob o RGPD, e no uso de seus poderes de aplicação do código.

O código também pode ser aplicado às provas nos processos judiciais, e os tribunais devem levar em conta suas disposições sempre que for relevante.

O que acontece se não estivermos em conformidade com os parâmetros deste código?

Se você não estiver em conformidade com os parâmetros deste código, provavelmente terá mais dificuldade em demonstrar que seu tratamento de dados é leal e que está em conformidade com o RGPD e o RPCE. Se você tratar os dados pessoais de uma criança de forma a violar o previsto pelo RGPD ou pelo RPCE, medidas regulatórias serão cabíveis.

As ferramentas à nossa disposição incluem aviso de avaliação[10], advertências, repreensões, notificações de execução e notificações de penalidades (multas administrativas). Para violações graves dos princípios de proteção de dados, temos o poder de emitir multas de até 20 milhões de euros (£17,5 milhões, quando o RGPD do Reino Unido entrar em vigor) ou 4% de seu faturamento anual global, a depender do valor que for mais alto.

Nossa abordagem para usar esses poderes levará em conta os riscos a que foram expostas as crianças após o tratamento de dados, assim como o esforço feito para se adequar aos parâmetros deste código. Se encontrarmos algo contra você, a probabilidade de lhe conceder tempo para adequar o seu serviço e deixá-lo em conformidade com o código será maior caso tenha fundamentos bem documentados que apoiem a sua bordagem.

Em contrapartida, se você não tiver tomado as medidas adequadas para estar em conformidade com o código, apesar das provas claras ou do conhecimento construtivo de que é provável que as crianças tenham acesso ao seu serviço e das provas evidentes de riscos significativos decorrentes do uso dos dados das crianças, é mais provável que tomemos medidas regulatórias formais. A abordagem estabelecida pela ICO para a execução deste código, conforme estabelecido em nossa Política de Ação Regulatória, aplicar-se-á ao uso de dados pessoais de crianças regulado sob RGPD e à consideração deste código.

Para mais informações, acessar a seção à parte sobre execução e cumprimento deste código.

10. NT. Um aviso de avaliação confere à ICO poderes excepcionais. Pode exigir que um controlador ou processador permita que a ICO entre nas instalações, seja direcionado para documentos e equipamentos, examiná-los, receba cópias e explicações, observe o processamento e entreviste o pessoal. In: https://www.lawsociety.org.uk/topics/gdpr/gdpr-in-practice-ico-enforcement-powers

Como este código será afetado com a saída do Reino Unido da União Europeia?

Este código se baseia e se refere às disposições relevantes da DPA 2018 e do RGPD, conforme se aplicam ao Reino Unido, em novembro de 2019, antes do dia de sua saída.

Se o Reino Unido deixar a UE sem nenhum acordo, a versão da UE do RGPD não será mais lei no Reino Unido. Entretanto, uma versão britânica do RGPD será inscrita na legislação britânica (UK RGPD). O RGPD do Reino Unido acompanhará uma versão emendada da DPA de 2018. Embora este código seja baseado nas disposições da DPA de 2018 e do RGPD da UE em vigor antes do dia de saída, os princípios, os direitos e as obrigações fundamentais de proteção de dados subjacentes a este código permanecerão os mesmos sob o RGPD do Reino Unido.

Os parâmetros deste código ainda serão, portanto, aplicáveis. A Autoridade continuará a levar o código em consideração. Entretanto, após o dia de saída, você deve ler as referências neste código ao RGPD, como referências à disposição equivalente no RGPD do Reino Unido. Também destacamos algumas mudanças específicas ao longo deste código, quando relevantes.

Se o Reino Unido concordar em deixar a UE com um acordo, haverá um período de implementação durante o qual o RGPD – e este código – continuará a ser aplicado no Reino Unido, da mesma forma que antes do dia da saída. No final do período de implementação, a situação padrão é a mesma que para uma saída sem acordo, e é esperado que este código permaneça em vigor.

Se houver qualquer outra mudança nos detalhes do futuro regime britânico, a Autoridade revisará os parâmetros deste código, a fim de que permaneçam relevantes e apropriados para apoiar o cumprimento da lei do Reino Unido.

Qual é o status das ‘leituras adicionais' ou de outros recursos vinculados?

Qualquer outra leitura ou outros recursos mencionados neste código ou ligados a ele não fazem parte do código. Disponibilizamos links para lhe dar contexto útil e orientações adicionais sobre questões específicas, mas não há nenhuma obrigação legal, descrita na DPA 2018, para que a Autoridade ou os tribunais a levem em consideração (a menos que seja um outro código legal de práticas).

Quando nos referimos a outras orientações da ICO, essas orientações inevitavelmente refletirão os pontos de vista da Autoridade e informarão sobre a nossa abordagem geral em relação a interpretação, conformidade e execução.

Também podemos nos vincular a orientações relevantes fornecidas pelo Comitê Europeu para a Proteção de Dados (CEPD), que é o órgão independente estabelecido para assegurar a coerência dentro da UE, ao interpretar o RGPD e ao tomar medidas regulatórias.

Como devemos usar o código?

Os parâmetros no início deste código são os 15 principais "parâmetros de *design* adequados à idade" que você precisa implementar. Este código é dividido em 15 seções, cada uma dando mais detalhes sobre o que significa cada parâmetro, a sua importância e como você pode implementá-lo. Esta explicação adicional é projetada para ajudá-lo, se você não tiver certeza do que fazer, mas não é taxativa. Ela deve lhe dar flexibilidade suficiente para desenvolver serviços que estejam de acordo com os parâmetros à sua própria maneira, adotando uma abordagem proporcional e baseada em riscos. Os parâmetros vão ajudar no *design* de serviços que estejam em conformidade com o RGPD e o RPCE.

Sua conformidade com o código será avaliada de acordo com os 15 parâmetros principais. No entanto, recomendamos que você leia o código na íntegra, pois ele o ajudará a compreender como você pode implementar cada padrão adequadamente. Essas normas são cumulativas e interdependentes – você deve implementá-las todas, na medida em que sejam relevantes ao seu serviço, a fim de demonstrar sua adequação ao código.

Este código pressupõe uma familiaridade com os principais termos e conceitos de proteção de dados. Incluímos um glossário, no final deste código, como um ponto de referência para conceitos e abreviações comuns, contudo, se você precisar de uma introdução à proteção de dados – ou mais contexto e orientação sobre conceitos-chave – você deve consultar nosso Guia de Proteção de Dados.

Este código se concentra em salvaguardas específicas para assegurar que seu regime de dados seja apropriado para crianças que, provavelmente, terão acesso ao seu serviço, para que você possa tratar seus dados de forma justa. O objetivo deste código não é o de ser um guia exaustivo para a conformidade com a proteção de dados. Por exemplo, ele não elabora sobre as suas obrigações em termos de segurança, operadores ou relatórios de violação. Você precisa ter certeza de que está ciente de todas as suas obrigações e deve ler este código junto com nossas outras orientações. Seu processo de RIPD deve incorporar medidas para cumprir com suas obrigações de proteção de dados em geral, bem como estar em conformidade com as normas específicas deste código.

Para leituras que vão além deste código:

- Convenção das Nações Unidas sobre os Direitos da Criança
- Guia de Proteção de Dados
- Guia para os Regulamentos de Privacidade e Comunicações Eletrónicas (Diretiva da CE) de 2003 (RPCE)
- Política de Ação Regulamentar da ICO
- Proteção de Dados e o Brexit

SERVIÇOS ABRANGIDOS POR ESTE CÓDIGO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

De forma resumida:

Este código se aplica aos"serviços da sociedade de informação que são de provável acesso por crianças" no Reino Unido. Isso inclui muitos aplicativos, programas, brinquedos e dispositivos conectados, mecanismos de busca, plataformas de mídia social, serviços de *streaming*, jogos on-line, notícias ou sites educacionais e sites que oferecem outros bens ou serviços aos usuários, através da internet. Não se restringe a serviços especificamente dirigidos às crianças.

De forma mais detalhada:

- A quais serviços este código se aplica?
- O que significa um 'serviço da sociedade de informação (SSI)'?
- Que tipos de serviços on-line não são considerados como 'SSI relevantes'?
- Quando os serviços são considerados de 'provável acesso por crianças'?
- É aplicável a serviços localizados fora do Reino Unido?
- E quanto aos regulamentos de comércio eletrônico de 2002?

A quais serviços este código se aplica?

A seção 123, da DPA 2018, estabelece que este código se aplica a:

> "serviços relevantes de sociedade da informação que são de provável acesso por crianças."

A DPA 2018 determina que 'serviços da sociedade de informação' têm o mesmo significado que no RGPD, com exceção de que não inclui 'serviços preventivos ou de aconselhamento', e que 'SSI relevantes' são aqueles que envolvem o tratamento de dados pessoais aos quais o RGPD se aplica.

A maioria dos serviços on-line usados por crianças encontram-se previstos no presente código, embora existam algumas exceções que são discutidas de forma mais detalhada abaixo. O Anexo A deste código fornece um fluxograma com as perguntas que você precisará responder, caso tenha dúvidas se seu serviço está abrangido pelo código ou não.

O que significa um 'serviço da sociedade de informação'?

A definição é ampla e a maioria dos serviços on-line que as crianças utilizam e acessam estão por ela abrangidos.

Um 'serviço da sociedade de informação' é definido como:

> "qualquer serviço normalmente prestado à distância, por meios eletrônicos, mediante remuneração e a pedido individual do destinatário.

Para efeitos desta definição:

> 1. 'à distância' significa que o serviço é prestado sem que as partes estejam simultaneamente presentes;
>
> 2. 'por meios eletrônicos' significa que o serviço é enviado inicialmente e recebido em seu destino por meio de equipamentos eletrônicos para o tratamento (incluindo compressão digital) e armazenamento de dados, e é inteiramente transmitido, transportado e recebido por fio, rádio, meios ópticos ou outros meios eletromagnéticos;
>
> 3. 'a pedido individual do destinatário' significa que o serviço é prestado através da transmissão de dados a pedido individual".

Isso significa que a maioria dos serviços on-line são SSI, incluindo aplicativos, programas e muitos sites, motores de busca, plataformas de mídia social, mensagens on-line ou serviços de telefonia de voz baseados na internet, mercados on-line, serviços de *streaming* de conteúdo (por exemplo, serviços de vídeo, música ou jogos), jogos on-line, notícias ou sites educacionais, e quaisquer sites que ofereçam outros bens ou serviços aos usuários através da internet. Serviços eletrônicos para controle de brinquedos conectados e outros dispositivos conectados também são considerados como SSI.

Esses serviços são incluídos ainda que a 'remuneração' ou o financiamento do serviço não venham diretamente do usuário final. Por exemplo, um aplicativo de jogos on-line ou motor de busca que é fornecido gratuitamente ao usuário final, mas financiado através de publicidade, ainda está dentro da definição de um SSI. Este código também abrange aplicativos sem fins lucrativos, jogos e sites educacionais, desde que esses serviços possam ser considerados como 'atividade econômica' em um sentido mais geral. Por exemplo, são tipos de serviços que normalmente são fornecidos em uma base comercial.

Se você é uma pequena empresa com um site, seu site será considerado como um SSI se você vende seus produtos on-line ou oferece um tipo de serviço que é transacionado, única ou predominantemente, através de seu site, sem que você precise passar tempo com o cliente pessoalmente.

Que tipos de serviços on-line não são considerados como 'SSI relevantes'?

Alguns serviços prestados pelas autoridades públicas

Se você é uma autoridade pública que fornece um serviço público on-line, então, desde que o tipo de serviço que você oferece não seja normalmente fornecido em uma base comercial, seu serviço não é um SSI relevante. Isso porque não é um serviço 'normalmente prestado mediante remuneração'.

Se você é uma força policial ou outra autoridade competente com um serviço on-line que processa dados pessoais para fins de execução da lei, então seu serviço não é um SSI relevante. Isso porque os SSI relevantes são aqueles que envolvem o tratamento de dados pessoais 'ao qual se aplica o RGPD'. O RGPD não se aplica ao tratamento pelas autoridades competentes, para fins de execução da lei. Para mais informações sobre o escopo do RGPD e como a lei de proteção de dados se aplica ao tratamento para fins de cumprimento da lei, consulte nosso Guia de proteção de dados.

Sites que fornecem apenas informações sobre um negócio ou um serviço que ocorre no mundo físico

Se seu site fornece apenas informações sobre seus negócios no mundo físico, mas não permite aos clientes comprar produtos on-line ou acessar um serviço on-line específico, ele não é um SSI. Isso porque o serviço oferecido não é fornecido 'à distância'. Um serviço de reservas on-line para uma consulta presencial não se qualifica como um SSI.

Serviços de telefonia tradicionais

Os serviços de telefonia tradicionais não são SSI relevantes, porque não são considerados como 'entregues por meios eletrônicos'. Isso difere dos serviços de telefonia de voz baseados na internet (VOIP) que estão dentro do escopo, pois são entregues pela internet por meios eletrônicos.

Serviços gerais de transmissão

A definição de um SSI não inclui serviços de transmissão como transmissões programadas de televisão ou rádio que são transmitidas para uma audiência geral, e não a pedido do indivíduo (mesmo que o canal seja transmitido através da internet).

Isso difere dos serviços 'sob demanda', que, por sua natureza, são prestados a pedido individual de um destinatário.

Se você fornecer tanto uma transmissão geral, quanto um serviço sob demanda, então o elemento 'sob demanda' de seu serviço será abrangido pelo código.

Serviços preventivos ou de aconselhamento

Este código não se aplica a sites ou aplicativos que oferecem aconselhamento on-line ou outros serviços preventivos (como exames de saúde ou check-ups) para crianças. Isso se deve ao fato de que a seção 123 não inclui os serviços de prevenção ou aconselhamento'. No entanto, aplicações ou serviços mais gerais de saúde, *fitness* ou bem-estar estão incluídos.

Quando os serviços são considerados de 'provável acesso por crianças'?

Este código se aplica se for provável que crianças acessem o seu serviço. De acordo com a CNUDC e para os fins deste código, uma criança é definida como uma pessoa menor de 18 anos.

Se o *design* de seu serviço for voltado especificamente para menores de 18 anos, então o código se aplica. Porém, a disposição da seção 123 da DPA é mais ampla do que isso. Ela também se aplica a serviços que não são, especificamente, destinados ou dirigidos a crianças, mas que são de provável acesso por menores de 18 anos.

É importante considerar que o Parlamento adotou a expressão de 'provável acesso por', em vez de termos mais restritos para garantir que a aplicação do código não excluísse os serviços que as crianças estavam de fato utilizando. Essa escolha teve como base a experiência de outros regimes internacionais de proteção à criança on-line, que se concentraram apenas em serviços desenvolvidos para crianças e, portanto, deixaram uma lacuna em sua incidência, gerando um maior risco.

Consideramos que, para que um serviço seja 'provável' de ser acessado, a possibilidade de que isso aconteça precisa ser mais provável do que não provável. Assim, reconhecemos a intenção do Parlamento de abranger os serviços que as crianças utilizam de fato, mas não ampliamos a definição para abranger todos os serviços aos quais as crianças poderiam eventualmente ter acesso.

Na prática, a probabilidade de o seu serviço ser acessado por crianças ou não, provavelmente, dependerá da:

- natureza e do conteúdo do serviço, e se isso gera um apelo particular para as crianças; e

- forma como o serviço é acessado de quaisquer medidas tomadas para impedir que as crianças consigam esse acesso.

Você deve adotar o bom senso na abordagem dessa pergunta. Se o seu serviço é do tipo que você não gostaria que as crianças acessassem em hipótese alguma, então seu foco deve estar em como impedir ou evitar o acesso (caso em que este código não se aplica), ao invés de torná-lo acessível às crianças (*child-friendly*). Por exemplo, se for um serviço somente para adultos, restrito ou, de outra forma, impróprio para crianças. Este código não deve conduzir ao resultado perverso de provedores de serviços restritos terem que tornar seus serviços acessíveis às crianças (*child-friendly*).

Se o seu serviço não for direcionado às crianças, mas também não for inadequado para que elas o utilizem, então seu foco deve ser a avaliação de o quanto seu serviço será atraente para elas. Se a natureza, o conteúdo ou a apresentação de seu serviço o faz pensar que as crianças vão querer usá-lo, então você deve estar em conformidade com os parâmetros deste código.

Se você tiver um serviço existente e as crianças formarem um grupo de usuários significativo e identificável, a definição 'provável de ser acessado por' será aplicada.

Dada a abrangência da aplicação, a ICO considera que será possível cumprir com este código de forma proporcional e baseada em riscos.

Se você decidir que o seu serviço não será de provável acesso por crianças e que, portanto, não vai implementar o código, então você deve documentar e justificar as razões para a sua decisão. Talvez seja interessante consultar pesquisas de mercado, evidências atuais sobre o comportamento dos usuários, a base de usuários de serviços similares ou existentes e os tipos de serviços e testes de medidas de restrição de acesso.

Se você julgar, inicialmente, que não é provável que o serviço seja acessado por crianças, mas mais tarde surgirem provas de que existe um número significativo de crianças que estão de fato acessando seu serviço, você precisará estar em conformidade com os parâmetros deste código ou rever suas restrições de acesso, caso não considere ser adequado que crianças acessem o seu serviço.

É aplicável a serviços localizados fora do Reino Unido?

Este código é emitido sob a DPA 2018. A DPA 2018 se aplica aos serviços on-line baseados no Reino Unido.

Também se aplica aos serviços on-line baseados fora do Reino Unido que possuem uma filial, um escritório ou um outro 'estabelecimento' no Reino Unido e processam dados pessoais no contexto das atividades daquele estabelecimento.

A DPA 2018 também pode se aplicar a alguns outros serviços baseados fora do Reino Unido, mesmo que eles não tenham um estabelecimento no Reino Unido. Se o estabelecimento relevante estiver fora do Espaço Econômico Europeu (EEE), a DPA 2018 ainda se aplica se você oferecer o serviço a usuários no Reino Unido ou monitorar o comportamento dos usuários no Reino Unido. O código se aplica se o serviço em questão for de provável acesso por crianças.

Se você não tem um estabelecimento no Reino Unido, mas tem um estabelecimento em outro lugar na EEE, este código não se aplica (mesmo que você ofereça seu serviço aos usuários do Reino Unido ou monitore o comportamento dos usuários no Reino Unido).

Se o código se aplicar ao seu tratamento, mas, de acordo com o mecanismo "*one-stop-shop*" do RGPD[11], você tem uma autoridade de supervisão principal que não a ICO, então podemos pedir a eles que levem o código em consideração, ao avaliar sua conformidade com o RGPD e o RPCE. Alternativamente, se considerarmos como um caso 'local' (afetando apenas usuários do Reino Unido), podemos tomar medidas próprias e aplicar o presente código.

Como isso será alterado quando o Reino Unido deixar a UE?

Quando o Reino Unido deixar a UE (ou no final do período de implementação, se o Reino Unido deixar a UE com um acordo), o regime britânico se aplicará aos serviços estabelecidos na EEE que estão buscando usuários britânicos, da mesma forma que aos serviços estabelecidos fora da EEE. O Reino Unido não fará mais parte do mecanismo "*one-stop-shop*" previsto pelo RGPD.

Se você estiver estabelecido na EEE e oferecer seu serviço aos usuários do Reino Unido ou monitorar o comportamento dos usuários no Reino Unido, este código será aplicado a você a partir do dia de saída (ou a partir do final do período de implementação, se um acordo for realizado).

---

11. O *One-stop-shop* é um mecanismo de caráter supranacional, criado pelo Regulamento nº 2016/679 (Regulamento Geral Europeu sobre a Proteção de Dados, o RGPD), que objetiva a resolução de litígios relacionados ao tratamento transfronteiriço de dados pessoais na União Europeia (UE). Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/one-stop-shop-o-novo-sistema-de-resolucao-de-litigios-da-uniao-europeia-22012021#:~:text=O%20One%2Dstop%2Dshop%20%C3%A9,na%20Uni%C3%A3o%20Europeia%20(UE)>. Acesso em 21 de maio de 2021.

E quanto aos regulamentos de comércio eletrônico de 2002?

Os Regulamentos de Comércio Eletrônico 2002 (RCE) não o isentam do cumprimento de suas obrigações de proteção de dados. O Regulamento 3(1)(b), do RCE, conforme emendado pelo Anexo 19, Parte 2, parágrafo 288, do DPA 2018, estabelece que:

> "Estes regulamentos e os seus conteúdos não são aplicáveis em relação a...
>
> (b) questões relativas aos serviços da sociedade da informação abrangidos pelo GDPR e pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativo ao tratamento de dados pessoais e à proteção da privacidade, no setor das comunicações eletrônicas (Diretiva sobre privacidade e comunicações eletrônicas)".

Embora o RCE inclua um regime de 'porto seguro' (*safe harbor*) para certas atividades que você possa realizar como prestador de serviços 'intermediário', é importante observar que:

- isso não elimina sua responsabilidade pelo cumprimento da proteção de dados, seja em geral ou em relação a essas atividades; e
- as disposições do RGPD não obstam este regime.

A ICO levará em consideração o regime de 'porto seguro', particularmente nos casos de reclamações e possíveis ações regulatórias decorrentes de atividades relacionadas àquelas que o regime de 'porto seguro' abrange.

Você deve avaliar como a estrutura legal se aplica às atividades que você executa por direito próprio e aquelas que você executa como intermediário. Por exemplo, um provedor de serviços de Internet (ISP) ou um operador de rede móvel (MNO) pode fornecer serviços centrais de conectividade como um provedor de serviços intermediário, enquanto também fornece serviços como aplicativos de atendimento ao cliente ou sites corporativos. Se necessário, você terá que recorrer a um aconselhamento jurídico especializado.

Para mais informações, consulte a seção sobre a 'Obrigação de Cumprimento deste código'.

Para leituras que vão além deste código:

Para mais informações sobre a definição de serviços da sociedade de informação (SSI), acesse:

- Artigo 1(1) e Anexo 1 da Diretiva (UE) 2015/1535 (Artigo 4(25) do RGPD incorpora essa definição ao RGPD)

- Ker-Optika vs ANTSZ (CJEU caso C-108/09, 2 dezembro de 2010)
- McFadden vs Sony (CJEU caso C-484/14, 15 setembro de 2016)
- Elite Táxi vs Uber (Parecer do Procurador Geral no caso C-434/15, 11 de maio de 2017)

Para mais informações sobre a aplicabilidade do RGPD, acesse:

- Introdução à Proteção de Dados - Qual regime aplicar?

Para mais informações sobre o princípio *one-stop-shop*, acesse:

- Diretrizes da CEPD sobre a autoridade supervisora principal.

A ICO iniciou uma consulta sobre um programa de apoio para os fornecedores de serviços on-line que são de provável acesso por crianças.

DISPOSIÇÕES TRANSITÓRIAS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

De forma resumida:

Os provedores de serviços da sociedade de informação (SSI) cujos serviços são considerados de provável acesso por crianças devem alinhar seu tratamento aos parâmetros deste código até 2 de setembro de 2021.

De forma mais detalhada:

- Quando este código entrará em vigor?
- O que deve ser feito a respeito de serviços já existentes?

Quando este código entrará em vigor?

O código foi publicado em 12 de agosto de 2020.

Ele entra em vigor em 2 de setembro de 2020.

A partir de 2 de setembro de 2021, a Autoridade deve observar o que dispõe o código, ao considerar se um serviço on-line cumpriu com suas obrigações de proteção de dados nos termos do RGPD e do RPCE. Os tribunais também devem levar em conta a disposição do código, quando relevante, a partir dessa data.

Nossa abordagem é a de incentivar a conformidade e gostaríamos de encorajá-lo a começar a se preparar para a entrada em vigor do código o quanto antes. De acordo com nossa Política de Ação Regulatória, ao considerar qualquer ação de execução, levaremos em consideração os esforços feitos para estar em conformidade durante o período de transição, bem como o tamanho e os recursos de sua organização, e os riscos para as crianças inerentes ao tratamento de seus dados.

O código será aplicado tanto aos serviços novos como aos já existentes.

O que deve ser feito a respeito de serviços já existentes?

Recomendamos que você comece fazendo uma revisão de seus serviços existentes, para estabelecer se eles estão abrangidos.

Para os serviços que já estão abrangidos, você já deve ter um RIPD (relatório de impacto à proteção de dados pessoais) – que agora deve ser revisado (ou, a depender da situação, elaborar um novo relatório) o

mais rápido possível. Isso lhe dará o máximo de tempo disponível para adequar seu tratamento aos parâmetros do código. Você deve concentrar-se em avaliar a conformidade com os parâmetros deste código e identificar quaisquer medidas adicionais necessárias para a adequação e o cumprimento.

Você deve efetuar as alterações em seu serviço o mais rápido possível e, no máximo, até o dia 2 de setembro de 2021.

Quando as mudanças incluírem mudanças em produtos físicos, em vez de produtos exclusivamente on-line, você deve assegurar-se de que as mudanças necessárias sejam incorporadas nos cronogramas de ciclos de fabricação iniciados após 2 de setembro de 2021. Por exemplo, se você estiver fazendo alterações nas embalagens, nas informações impressas ou no componente físico de um brinquedo ou um dispositivo conectado, você não será obrigado a retirar ou alterar estoque existente ou ciclos de fabricação que já estavam programados para começar antes de 2 de setembro de 2021, quando este código entra em vigor.

Você também deve considerar como gerenciar quaisquer mudanças na forma como seu serviço funciona com seus usuários existentes. Você deve pensar em como a experiência on-line deles pode mudar e como melhor comunicar-lhes e prepará-los para essas mudanças, a fim de que qualquer impacto seja gerenciado adequadamente.

PARÂMETROS DE *DESIGN* ADEQUADOS À IDADE

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

A seção 123 da DPA 2018 determina que este código deve incluir:

> "orientações que a Autoridade julgar importante sobre padrões de *design* adequados à idade, em relação a serviços da sociedade de informação que são de provável acesso por crianças."

Define-se parâmetros de *design* adequados como:

> "padrões de *design* adequados à idade, cujos serviços a que estão relacionados, a Autoridade entenda como necessários, para cumprir o melhor interesse das crianças."

Os parâmetros não são concebidos como padrões técnicos, mas sim como um conjunto de princípios de *design* tecnológicos neutros que contam com recursos práticos de privacidade. O foco deste código é estabelecer um benchmark[12] para a proteção adequada dos dados pessoais de crianças. Portanto, serviços diferentes exigirão soluções técnicas distintas.

Você deve incorporar os parâmetros estabelecidos neste código em seus processos de *design* desde o início, em processos subsequentes de atualização e desenvolvimento de serviços e em seu RIPD.

Para mais informações sobre como aplicamos esses parâmetros, consulte a seção separada sobre a obrigação de execução deste código.

12. NT "(...) benchmark é o ato de comparar de forma eficiente a performance entre dispositivos utilizando um ou mais programas. Para conseguir compará-los de maneira equivalente, é preciso realizar uma série de testes e analisar inúmeros dados diferentes.". Disponível em: <https://canaltech.com.br/hardware/o-que-e-benchmark-26350/#:~:text=No%20universo%20da%20computa%C3%A7%C3%A3o%2C%20benchmark,e%20analisar%20in%C3%BAmeros%20dados%20diferentes. > Acesso em 21 de maio de 2021.

1. O MELHOR INTERESSE DA CRIANÇA

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> O melhor interesse da criança deve ser uma consideração primordial para o *design* e o desenvolvimento on-line de seus serviços de provável acesso por crianças.

O que se quer dizer com 'o melhor interesse da criança'?

O conceito de melhor interesse da criança decorre do Artigo 3, da Convenção das Nações Unidas sobre os Direitos da Criança (CNUDC):

> "Todas as ações relativas à criança, sejam elas levadas a efeito por instituições públicas ou por privadas de assistência social, tribunais, autoridades administrativas ou órgãos legislativos, devem considerar primordialmente o melhor interesse da criança."

A CNUDC incorpora disposições destinadas a auxiliar as necessidades da criança em termos de segurança, saúde, bem-estar, relações familiares, desenvolvimento físico, psicológico e emocional, identidade, liberdade de expressão, privacidade e capacidade para formar suas próprias opiniões e fazer com que elas sejam ouvidas. Em termos simples, o melhor interesse da criança é aquilo que for melhor para aquela criança específica.

A CNUDC reconhece, expressamente, o papel dos pais e dos responsáveis (incluindo a família estendida, tutores e outros com responsabilidade legal) na proteção e na promoção do melhor interesse da criança.

Também reconhece o direito da criança à privacidade e de ser protegida contra a exploração econômica. Além de também ressaltar a importância do acesso à informação, da associação com outras pessoas e do "brincar" no apoio ao desenvolvimento da criança. Ressalta também o direito da criança, de acordo com o desenvolvimento progressivo de suas capacidades, de ter voz em assuntos que a afetem.

A CNUDC fornece uma estrutura que equilibra uma série de interesses e preocupações diferentes, com a intenção de proporcionar o que for melhor para cada criança individualmente.

A classificação do melhor interesse da criança como 'consideração primordial' reconhece que o melhor interesse da criança tem que ser equilibrado com outros interesses. Por exemplo, o melhor interesse de

duas crianças distintas podem estar em conflito, ou agir unicamente no melhor interesse de uma criança pode prejudicar os direitos de outras. No entanto, é improvável que os interesses comerciais de uma organização prevaleçam sobre o direito à privacidade de uma criança.

Por que isso é importante?

Isso é importante porque a ICO é obrigada a levar em consideração as obrigações do Reino Unido submetidas à CNUDC, na elaboração deste código.

Também é importante porque proporciona uma estrutura para ajudar na compreensão das necessidades das crianças e dos direitos que precisam ser levados em conta ao elaborar o *design* de serviços on-line.

O Artigo 5(1)(a), do RGPD, determina que os dados pessoais são:

> "Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência')".

E o Considerando 38, do RGPD, determina que:

> "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais..."

Se você considerar o melhor interesse das crianças usuárias em todos os aspectos de seu *design* de serviços on-line, então terá maior facilidade em cumprir com o princípio de 'licitude, lealdade e transparência', e, devidamente, levar em consideração o previsto no considerando 38.

O princípio do 'melhor interesse da criança' é, portanto, um princípio que você precisa considerar especificamente ao desenvolver o *design* de seu serviço on-line e é também um tema que percorre todas as disposições deste código.

Como podemos ter certeza de que cumprimos este padrão?

Considerar e apoiar os direitos das crianças

Para implementar este padrão, você precisa considerar as necessidades dos usuários infantis e descobrir como você pode melhor apoiar essas necessidades no *design* de seu serviço on-line, ao tratar dados

pessoais. Ao fazer isso, você deve levar em conta a idade do usuário. Talvez seja necessário usar provas e conselhos de terceiros especialistas no assunto para melhor orientá-lo.

Em particular, você deve considerar, em seu uso de dados pessoais, como você pode:

- mantê-las a salvo de riscos de exploração, incluindo os riscos de exploração comercial ou sexual e de abuso sexual;
- proteger e apoiar a saúde e o bem-estar delas;
- proteger e apoiar o desenvolvimento físico, psicológico e emocional delas;
- proteger e apoiar as necessidades delas de desenvolver suas próprias visões e identidades;
- proteger o direito delas à liberdade de associação e de brincar;
- apoiar as necessidades das crianças com deficiência, de acordo com obrigações assumidas perante a legislação de igualdade relevante para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte;
- reconhecer o papel dos pais na proteção e na promoção do melhor interesse da criança e apoiá-los nessa tarefa; e
- reconhecer a capacidade em desenvolvimento progressivo da criança de formar sua própria visão/opinião, e dar o devido peso a essa visão/opinião.

Considerar o melhor interesse da criança não significa que você não possa buscar seus próprios interesses comerciais ou outros. Seus interesses comerciais podem não ser incompatíveis com o melhor interesse da criança, mas você precisa levar em conta o melhor interesse da criança como uma consideração primordial, quando surgir qualquer conflito.

Para mais informações além deste código:

- Convenção das Nações Unidas sobre os Direitos da Criança

2. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Realizar um RIPD para avaliar e mitigar os riscos aos direitos e às liberdades das crianças em decorrência do tratamento de seus dados devido ao provável acesso ao seu serviço. Considerar as diferentes idades, capacidades e necessidades de desenvolvimento e garantir que seu RIPD seja desenvolvido em conformidade com este código.

O que se quer dizer com um 'RIPD'?

Um RIPD é um processo definido para ajudá-lo a identificar e minimizar os riscos de proteção de dados de seu serviço – e, em particular, os riscos específicos para as crianças que provavelmente terão acesso a seu serviço, decorrentes do tratamento de seus dados pessoais.

Você deve realizar um RIPD ao iniciar o *design* do seu serviço, antes de começar o seu tratamento de dados. Deve incluir as seguintes etapas:

- Etapa 1: identificar a necessidade de um RIPD
- Etapa 2: descrever o tratamento
- Etapa 3: considerar uma consultoria
- Etapa 4: avaliar a necessidade e a proporcionalidade
- Etapa 5: identificar e avaliar os riscos decorrentes de seu tratamento
- Etapa 6: identificar medidas para mitigar os riscos
- Etapa 7: finalizar a sessão, registrar e integrar os resultados

O processo do RIPD é projetado para ser flexível e escalável[13]. Você pode desenvolver um processo que se adapte à sua abordagem existente de *design* e desenvolvimento, desde que contenha esses elementos-chaves e que os resultados influenciem o *design* de seu serviço. Não precisa ser um processo demorado em todos os casos.

Para mais informações além deste código:

Acesse o nosso guia detalhado sobre RIPDs.

13. A escolha para o uso da palavra "escalável" se deu em razão de que, no âmbito de sistemas eletrônicos, existe a expressão "Sistema Escalável". "Escalabilidade é a capacidade que um Sistema possui para gerenciar uma quantidade elevada de processos ou o potencial para elevar a largura de tratamento, a fim de acomodar o crescimento de tarefas".

Por que os RIPDs são importantes?

Os RIPDs são uma parte fundamental de suas responsabilidades em relação ao RGPD, e ajudam você a adotar uma abordagem de 'proteção de dados desde concepção e como padrão'. Um bom RIPD também é uma forma eficaz de avaliar e documentar o cumprimento de todas as suas obrigações de proteção de dados e das disposições deste código.

O RGPD determina que você deve realizar um RIPD antes de iniciar **qualquer tipo de tratamento que possa resultar em um alto risco** para os direitos e as liberdades dos indivíduos.

A questão não é se o seu serviço é realmente de alto risco, mas sobre a triagem de potenciais indicadores de alto risco. A natureza e o contexto dos serviços on-line, no âmbito deste código, significam que eles inevitavelmente envolvem um tipo de tratamento suscetível de resultar em um alto risco para os direitos e as liberdades de crianças.

A ICO é obrigada, pelo artigo 35(4), do RGPD, a publicar uma lista das operações de tratamento que requerem um RIPD. Essa lista complementa os critérios do RGPD e as diretrizes europeias relevantes, assim como inclui:

> "o uso dos dados pessoais de crianças ou de outros indivíduos vulneráveis para fins de marketing, perfilamento ou outras decisões automatizadas, ou se você pretende oferecer serviços on-line diretamente às crianças".

Os serviços on-line também podem desencadear vários outros critérios que indicam a necessidade de um RIPD, incluindo tecnologia inovadora, perfilamento em larga escala, dados biométricos e rastreamento on-line. Na prática, isso significa que, se você oferece um serviço on-line que será de provável acesso por crianças, você precisa fazer um RIPD.

No entanto, os RIPDs não são apenas um exercício de conformidade. Seus RIPDs devem considerar os riscos de conformidade, mas também riscos mais amplos aos direitos e às liberdades das crianças que possam surgir do tratamento de dados, inclusive o potencial surgimento de quaisquer danos materiais, físicos, psicológicos ou sociais significativos.

Um RIPD eficaz permite identificar e corrigir problemas em um estágio inicial, desenvolvendo a proteção de dados desde o início. Isso pode trazer economia de custos e benefícios mais amplos, tanto para as crianças, quanto para sua organização. Pode assegurar aos pais que você protege os interesses de seus filhos e que seu serviço é adequado para

crianças. A fase de consulta de um RIPD também pode dar às crianças e aos pais a chance de opinar sobre como seus dados são utilizados, ajudar a construir confiança e melhorar sua compreensão das necessidades, preocupações e das expectativas específicas das crianças. Também pode ajudar a evitar danos à sua reputação mais tarde.

Como ter certeza de que este padrão foi cumprido adequadamente?

Não há um modelo definitivo de RIPD, mas você pode usar ou adaptar o modelo incluído como anexo a este código, se desejar.

Você deve consultar seu encarregado pelo tratamento de dados pessoais, internacionalmente conhecido como *Data Protection Officer* (DPO), se tiver um, e, quando apropriado, indivíduos e especialistas relevantes. Outros operadores também podem precisar ajudá-lo.

Seu RIPD deve ter como foco particular os direitos e os riscos que existem para crianças que utilizam seus serviços que surgem do tratamento de seus dados. Deve também avaliar e documentar sua conformidade com este código. Você deve incorporar esses elementos adicionais em cada etapa de seu RIPD, e não apenas incluí-los ao final.

Você precisa seguir o procedimento usual do RIPD estabelecido em nosso guia de orientação sobre como realizar um RIPD, assim como incluir as seguintes questões específicas em cada etapa.

Etapa 1: Identifique quando fazer seu RIPD

Você deve incorporar um RIPD no *design* de qualquer novo serviço on-line que seja de provável acesso por crianças. Você deve completar seu RIPD para que o serviço seja implementado e assegurar que os resultados possam influenciar seu *design*. Você não deve tratar um RIPD apenas como um carimbo ou um item a mais a ser marcado no final do processo de *design*.

Você também precisa fazer um RIPD se estiver planejando executar qualquer mudança significativa nas operações de tratamento de um serviço on-line existente de provável acesso por crianças.

Uma mudança externa que influencie o contexto do seu serviço também pode levá-lo a rever seu RIPD. Por exemplo, se uma nova falha de segurança for identificada ou se uma nova preocupação pública for levantada sobre características específicas de seu serviço ou riscos particulares para crianças.

Para mais informações além deste código:

Lista da ICO de operações de tratamento que requerem um RIPD

Diretrizes europeias sobre RIPDs

Etapa 2: Descrição do tratamento

Você precisa descrever a natureza, o escopo, o contexto e os objetivos do tratamento. Especificamente, você deve incluir:

- se você está desenvolvendo seu serviço para crianças;
- em caso negativo, se é provável que as crianças tenham acesso a seu serviço;
- a faixa etária dessas crianças;
- seus planos, se houver, para um controle parental;
- seus planos, se houver, para estabelecer a idade de seus usuários individuais;
- os benefícios esperados para as crianças;
- os interesses comerciais (seus ou de terceiros) que foram levados em consideração;
- qualquer perfilamento ou qualquer tomada de decisão automatizada envolvida;
- quaisquer elementos de geolocalização;
- o uso de qualquer técnica de *nudge*;
- qualquer tratamento de dados de categoria especial;
- qualquer tratamento de dados inferidos;
- quaisquer questões atuais de interesse público sobre riscos on-line para crianças;
- quaisquer padrões ou códigos de prática relevantes do setor;
- suas responsabilidades de acordo com a legislação de igualdade aplicável à Inglaterra, à Escócia, ao País de Gales e à Irlanda do Norte; e
- qualquer orientação ou qualquer pesquisa relevante sobre as necessidades de desenvolvimento, bem-estar ou capacidade das crianças na faixa etária relevante.

Etapa 3: Consultar as crianças e os pais

Dependendo do tamanho de sua organização, dos recursos e dos riscos identificados, você pode buscar e documentar as opiniões das crianças e dos pais (ou de seus representantes), e levá-las em conta em seu *design*.

Esperamos que organizações de grande porte façam alguma forma de consulta. Por exemplo, você poderia optar por obter feedback dos usuários existentes, realizar uma consulta pública geral, conduzir pesquisas de mercado, realizar testes de usuários ou contatar grupos de direitos das crianças relevantes para suas opiniões. Isso deve incluir feedback sobre a capacidade da criança de compreender a forma como você utiliza seus dados e as informações que você fornece. Se você considerar que não é possível fazer qualquer forma de consulta, ou que isso seria desnecessário ou totalmente desproporcional, você deve registrar essa decisão em seu RIPD e estar preparado para justificá-la. Entretanto, geralmente é possível realizar alguma forma de pesquisa de mercado ou de feedback do usuário.

Você também deve considerar a possibilidade de buscar conselhos independentes de especialistas em direitos das crianças e suas necessidades de desenvolvimento como parte desta etapa. Isso é especialmente importante para os serviços:

- cujos designs são especificamente para crianças;
- cujos *designs* são para uso geral, mas conhecidos por serem amplamente utilizados por crianças (tais como jogos ou sites de mídia social); ou
- que utilizem os dados das crianças de maneiras novas ou imprevistas.

Etapa 4: Avaliar a necessidade, a proporcionalidade e a adequação (compliance)

Você precisa explicar por que seu tratamento é necessário e proporcional para seu serviço. Você também deve incluir informações sobre como você cumpre com o RGPD, inclusive:

- sua base legal para o tratamento (ver Anexo C);
- sua condição para o tratamento de quaisquer dados pessoais sensíveis;
- medidas para garantir a precisão, evitar preconceitos e explicar o uso de IA;
- e detalhes específicos de suas medidas de segurança tecnológicas (por exemplo, *standards* de *hashing* ou criptografia).

Além disso, nesta fase, você deve incluir uma explicação de como você está em conformidade com cada um dos parâmetros estabelecidos neste código.

Etapa 5: Identificar e avaliar os riscos

Você precisa considerar o potencial impacto nas crianças e qualquer dano ou prejuízo que seu tratamento de dados possa causar – seja físico, emocional, de desenvolvimento ou material. Você também deve avaliar, especificamente, se o tratamento pode causar, permitir ou contribuir para o risco de:

- danos físicos;
- aliciamento on-line ou outra exploração sexual;
- ansiedade social, problemas de autoestima, *bullying* ou pressão dos colegas;
- acesso a conteúdo nocivo ou inapropriado;
- desinformação ou restrição indevida de informações;
- incentivo à tomada de riscos excessivos ou comportamento insalubre;
- comprometimento da autoridade ou responsabilidade dos pais;
- perda de autonomia ou de direitos (incluindo o controle sobre dados);
- uso compulsivo ou distúrbios de déficit de atenção;
- tempo excessivo de tela;
- padrões de sono interrompidos ou inadequados;
- exploração econômica ou pressão comercial injusta; ou
- qualquer outra desvantagem econômica, social ou de desenvolvimento significativa.

Você deve ter em mente que as necessidades e a maturidade das crianças serão diferentes de acordo com suas idades e estágios de desenvolvimento. O Anexo B deve ajudar você a considerar isso.

Para avaliar o nível de risco, você deve considerar tanto a probabilidade, quanto a gravidade de qualquer impacto sobre as crianças. O alto risco pode resultar ou de uma alta probabilidade de algum dano, ou de uma menor possibilidade de dano grave. Você deve ter em mente que algumas crianças serão menos resistentes do que outras, portanto, você deve sempre adotar uma abordagem preventiva para avaliar a potencial gravidade do dano. Você pode descobrir que existe um alto risco para algumas faixas etárias, mesmo que o risco para outras seja menor.

Etapa 6: Identificar medidas para mitigar esses riscos

Você deve considerar se poderia fazer alguma mudança em seu serviço para reduzir ou evitar cada um dos riscos que você identificou. No mínimo, você deve implementar as medidas estabelecidas neste código, mas também deve considerar se pode colocar quaisquer salvaguardas adicionais como parte do *design* de seu serviço.

A transparência é importante. No entanto, você também deve identificar e considerar medidas que não dependam da capacidade ou da disposição das crianças de se envolverem com suas informações de privacidade.

Etapa 7: Registrar a conclusão

Se você tiver um DPO, deverá registrar seus conselhos independentes sobre o resultado do RIPD, antes de tomar qualquer decisão final.

Você deve registrar quaisquer medidas adicionais que planeja tomar e integrá-las ao *design* do seu serviço. Se você identificar um risco elevado que não esteja mitigando, você deve consultar a ICO, antes de avançar.

Publicar o seu RIPD é visto como uma boa prática.

Para mais informações além deste código:

Acesse o nosso guia detalhado sobre RIPDs.

3. APLICAÇÃO ADEQUADA À IDADE

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Adote uma abordagem baseada em riscos para reconhecer a idade de cada usuário e garantir que você aplique, efetivamente, os padrões deste código aos usuários infantis. Defina a idade com certo grau de confiança adequado para os riscos que podem surgir, em relação aos direitos das crianças, do tratamento de dados, ou implemente os padrões deste código a todos os seus usuários.

O que se quer dizer com 'aplicação adequada à idade'?

Isso significa que a faixa etária de seu público e as diferentes necessidades das crianças em diferentes idades e estágios de desenvolvimento devem estar no cerne da forma como você faz o *design* de seu serviço e aplica este código.

Isso também significa que você deve aplicar este código para que todas as crianças recebam um nível adequado de proteção na forma como seus dados pessoais são utilizados. Há flexibilidade para você decidir como aplicar este padrão no contexto e nas circunstâncias de seu serviço on-line. Isso geralmente significará estabelecer (com um nível de confiança adequado para os riscos que podem surgir, em relação aos direitos das crianças, do tratamento de dados) em qual faixa etária seus usuários individuais se enquadram, para que você possa adaptar as proteções e as salvaguardas de forma proporcional, aplicando os parâmetros deste código. Você deve usar o seu RIPD para fins de auxílio e avaliação para essas medidas.

Alternativamente, se não puder ou não quiser realizar estas medidas, você pode optar por aplicar os padrões a todos os seus usuários. Isto para que as crianças gozem de alguma protecção contra os riscos decorrentes da forma como os seus dados pessoais são utilizados, mesmo que não se esteja suficientemente certo de que sejam crianças ou não.

Por que isso é importante?

O objetivo final deste código é assegurar que os serviços on-line de provável acesso por crianças sejam adequados para seu uso e atendam às suas necessidades de desenvolvimento.

Compreender a faixa etária das crianças com probabilidade de acesso ao serviço – e as diferentes necessidades das crianças em dife-

rentes idades e estágios de desenvolvimento – é fundamental para todo o conceito de '*design* adequado à idade'.

As crianças são indivíduos e as faixas etárias não são um guia perfeito para os interesses, as necessidades e a capacidade de evolução de cada criança. Entretanto, para ajudá-lo a avaliar o que é adequado para crianças em geral, de acordo com a idade em que se encontram, você pode usar as faixas etárias como um guia para a capacidade, a habilidade e o comportamento que uma criança pode demonstrar em cada estágio de seu desenvolvimento. Para os fins deste código, usamos as seguintes faixas etárias e os seguintes estágios de desenvolvimento como um guia:

- 0 – 5: pré-alfabetização e alfabetização fundamental
- 6 – 9: principais anos da escola fundamental
- 10 – 12: anos de transição escolar
- 13 – 15: início da adolescência
- 16 – 17: aproximando-se da maioridade

Não há nenhuma exigência para que você desenvolva serviços para estágios de desenvolvimento que não são prováveis de acessar seu serviço ou usar exatamente essas faixas etárias, se você puder justificar o motivo pelo qual faixas etárias ligeiramente diferentes são mais adequadas para seu serviço específico.

Mais informações sobre capacidades, necessidades, habilidades e comportamentos relevantes em cada etapa são apresentadas no Anexo B deste código, para fins de referência e para que se apliquem, quando relevante, a cada um desses parâmetros .

Você também deve considerar as necessidades das crianças com deficiência de acordo com quaisquer obrigações que você possa ter sob a legislação de igualdade relevante para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

O RGPD e a DPA 2018 também especificam que, se você se basear no consentimento para qualquer aspecto de seu serviço on-line, você precisa obter autorização dos pais para crianças menores de 13 anos. Se você confiar no consentimento como sua base legal para tratar dados pessoais, então essas disposições têm implicações práticas significativas para você. O cumprimento dos parâmetros deste código deve permitir que você cumpra essas exigências do RGPD de forma proporcional. Acesse o Anexo C para mais detalhes.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Considere os riscos que surgem para as crianças resultantes do tratamento de dados e o nível de certeza que você tem sobre a idade de seus usuários.

- Você pode implementar este padrão ao seguir as etapas elencadas abaixo:
- Considere os riscos do tratamento dos dados pessoais para crianças. Seu RIPD o ajudará a fazer isso. Você pode querer levar em conta fatores como: os tipos de dados coletados; o volume de dados; a invasividade de qualquer tipo de perfilamento; se a tomada de decisão ou outras ações decorrem do perfilamento; e se os dados estão sendo compartilhados com terceiros. Tanto a ICO quanto o Comitê Europeu para a Proteção de Dados forneceram orientações sobre os RIPDs que indicam uma avaliação de risco mais detalhada.
- Considere o quanto você conhece seus usuários. O quão certo você está de que um usuário individual é um adulto ou uma criança? Até que ponto você está confiante quanto à faixa etária em que seus usuários individuais crianças se enquadram?
- Decida se o nível de certeza que você tem sobre a idade de seus usuários individuais é adequado para os riscos que surgem do tratamento de dados.
- Se for, então você pode aplicar os outros parâmetros deste código somente aos seus usuários crianças.
- Se não for, então decida se prefere:
  - » reduzir os riscos dos dados inerentes ao seu serviço;
  - » instituir medidas adicionais para aumentar seu nível de confiança na faixa etária que acessa os seus serviços;
  - » ou aplicar os parâmetros deste código a todos os usuários de seu serviço (independentemente de terem se autodeclarado como adultos ou como crianças).

Como podemos estabelecer a idade com um nível de certeza adequado?

Este código não é taxativo quanto aos métodos que você deve usar para estabelecer a idade, ou quanto ao nível de certeza que os diferentes métodos proporcionam. A razão para tanto é que isso varia

de acordo com as especificidades das técnicas que você utiliza. Queremos permitir flexibilidade suficiente para que você utilize medidas que se adaptem às especificidades de seu serviço individual e que possam se desenvolver ao longo do tempo. No entanto, você deve sempre usar um método adequado aos riscos que surgem do tratamento de dados de sua empresa.

Alguns dos métodos que você pode considerar estão listados abaixo. Essa lista não é exaustiva. Outras medidas podem existir ou surgir ao longo do tempo. Ao avaliar se você escolheu um método apropriado, levaremos em consideração os produtos atualmente disponíveis no mercado, particularmente para pequenas empresas que não têm recursos para desenvolver suas próprias soluções.

- **Autodeclaração -** Aqui é onde um usuário simplesmente declara sua idade, mas não fornece nenhuma evidência para confirmá-la. Ela pode ser adequada para tratamento de baixo risco ou quando usada em conjunto com outras técnicas. Mesmo que você prefira aplicar os parâmetros do código a todos os seus usuários, a autodeclaração de idade pode oferecer um ponto de partida útil ao fornecer informações de privacidade e explicações apropriadas sobre o tratamento (veja 'O que significa aplicar os parâmetros a todos os usuários na prática?' para obter mais detalhes).
- **Inteligência artificial -** Pode ser possível fazer uma estimativa de idade de um usuário usando a inteligência artificial para analisar a forma como o usuário interage com seu serviço. Da mesma forma, você poderia usar este tipo de perfilamento para verificar se a maneira como um usuário interage com seu serviço é consistente com sua idade autodeclarada. Esta técnica normalmente proporcionará um maior nível de certeza sobre a idade dos usuários com o aumento do uso de seu serviço. Se você optar por usar esta técnica, então você precisa:
  - » informar aos usuários sobre isso com antecedência;
  - » coletar apenas a quantidade mínima de dados pessoais necessárias para este fim;
  - » e não utilizar quaisquer dados pessoais coletados para este fim, para outros fins.
- **Serviços de verificação de idade de terceiros -** Você pode optar por utilizar um serviço de terceiros para fins de garantir a idade de seus usuários. Esses serviços normalmente funcionam em um sistema de 'atributos', nos quais você solicita confirmação de um determinado atributo do usuário (neste caso, idade ou faixa

etária) e o serviço lhe fornece uma resposta de 'sim' ou 'não'. Este método reduz a quantidade de dados pessoais que você precisa coletar e pode permitir que você tire proveito da experiência tecnológica e dos últimos desenvolvimentos na área. Se você usar um serviço de terceiros, precisará realizar algumas verificações de diligência para se certificar de que o nível de certeza com o qual confirma a idade é adequado (a norma PAS 1296 '*Online age checking*' pode ajudá-lo com isso) e que está em conformidade com os requisitos de proteção de dados. Você também deve fornecer aos seus usuários informações claras sobre o serviço que você utiliza.

- **Confirmação do titular da conta -** Você pode depender da confirmação de idade do usuário de um titular de conta já existente que você sabe que é um adulto. Por exemplo, se você fornecer um serviço baseado em login ou em assinatura, você pode permitir que o titular da conta principal (adulto confirmado) estabeleça perfis de crianças, restrinja o acesso adicional, com uma senha ou um PIN, ou simplesmente confirme a faixa etária de usuários adicionais da conta.
- **Medidas técnicas -** Medidas técnicas que desencorajam falsas declarações de idade, ou que identificam e fecham contas de menores de idade, podem ser úteis para auxiliar ou fortalecer os mecanismos de autodeclaração. Exemplos incluem a apresentação neutra de telas de declaração de idade (em vez de se referir à seleção de certas idades) ou o impedimento de que os usuários voltem a apresentar imediatamente uma nova idade, se lhes for negado o acesso ao seu serviço, quando autodeclararem pela primeira vez a sua idade.
- **Identificadores essenciais -** Você pode confirmar a idade usando soluções que remetam a documentos de identificação formais ou 'identificadores essenciais', como um passaporte, por exemplo. Entretanto, recomendamos que você evite deixar o usuário sem escolha, a não ser fornecer identificadores essenciais, a menos que os riscos inerentes ao seu tratamento realmente justifiquem essa abordagem. A razão para tanto reside no fato de que algumas crianças não têm acesso a documentos de identidade formais e podem ter apoio limitado dos pais, o que dificulta o acesso a serviços verificados por idade, mesmo que sejam apropriados para ela. A exigência de identificadores essenciais também pode ter um impacto desproporcional sobre a privacidade dos adultos.

Reconhecemos que os métodos de controle de idade variam de acordo com o uso do serviço por usuários autenticados ou não (por exemplo, se os usuários estão logados) e que os riscos também podem variar nesse contexto.

E se precisarmos coletar dados pessoais para estabelecer a idade?

Você pode coletar e registrar dados pessoaisque proporcionem uma garantia de idade de forma independente. Se assim for, lembre-se que você precisa cumprir com as obrigações de proteção de dados para sua coleta e sua retenção, incluindo minimização de dados, limitação de propósito, limitação de armazenamento e obrigações de segurança.

É fundamental que você colete somente a quantidade mínima de dados pessoais necessários para lhe dar um nível adequado de certeza sobre a idade de seus usuários individuais e que não utilize os dados pessoais coletados para efeitos de estabelecer ou de estimar a idade, visando à conformidade com este código, para outros fins.

Por exemplo, se você usar o perfilamento para ajudá-lo a estimar a idade de usuários individuais para que você possa aplicar os parâmetros deste código, então você pode usar essas informações para assegurar que você:

- providencie informações de privacidade, assim como utilize técnicas de *Nudge* adequadas à idade;
- providencie configurações de alta privacidade para usuários infantis por padrão; e;
- não forneça conteúdo considerado prejudicial à saúde e ao bem-estar das crianças.

Você não pode, no entanto, simplesmente, redirecionar essas informações para outros fins, como, por exemplo, fazer uma publicidade voltada às crianças para produtos que você acha que elas possam gostar ou enviar detalhes de ‘ofertas de aniversário’. Se você quiser fazer o perfilamento de crianças para esse fim, você precisa do consentimento delas. Consulte a seção deste código sobre perfilamento para obter mais detalhes.

Reconhecemos que existe uma tensão entre assegurar determinada idade e cumprir o RGPD, já que, ao implementar métodos que asseguram a idade, corre-se o risco de uma coleta de dados mais intrusiva. No entanto, não exigimos que as organizações criem esses riscos colaterais. Mas se forem usadas soluções de proteção de dados desde a concepção (*privacy by design*), será possível compatibilizar a necessidade de assegurar a idade e, ao mesmo tempo, cumprir com o RGPD.

As ferramentas usadas para assegurar a idade ainda são uma área em desenvolvimento. A autoridade apoiará o trabalho necessário para estabelecer parâmetros industriais claros e esquemas de certificação para auxiliar crianças, pais e serviços on-line na identificação de serviços que asseguram a idade e que estejam em conformidade com os parâmetros de proteção de dados.

Em termos práticos, o que significa aplicar os parâmetros a todos os usuários?

Se você não tiver um nível de confiança sobre a idade de seus usuários, adequado aos riscos para as crianças decorrentes do tratamento de dados, então sua alternativa é aplicar os parâmetros do código a todos os usuários. Isso significa que, mesmo que você não saiba realmente a idade de um usuário, ou se uma criança mentiu sobre sua idade, as crianças ainda receberão algumas proteções importantes na forma como seus dados pessoais são utilizados.

No entanto, isso não significa que você tenha que ignorar qualquer informação que tenha sobre a idade do usuário ou que os usuários adultos tenham que ser infantilizados. Significa apenas que todos os usuários receberão algumas proteções básicas na forma como seus dados pessoais são utilizados por padrão (*by default*).

Você deve aplicar os parâmetros deste código de forma a reconhecer, tanto as informações que você tem sobre a idade dos usuários, quanto o fato de que seu nível de confiança nessas informações é inadequado aos riscos inerentes ao seu tratamento. Por exemplo, fornecendo informações de privacidade adequadas à idade autodeclarada do usuário, mas lhes dando a opção de acessar versões escritas para diferentes faixas etárias também.

Para mais informações além deste código:

Acesse o nosso guia detalhado sobre RIPDs

Guia europeu sobre RIPDs

PAS 1296, Verificação on-line de idade - Código de Prática

4. TRANSPARÊNCIA

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Todas as informações de privacidade que são fornecidas aos usuários, assim como demais termos, políticas e padrões publicados, devem ser concisas, proeminentes e em linguagem clara e adequada à idade da criança. Devem ser fornecidas explicações adicionais específicas, chamadas de "*bite-size*", isto é, no sentido de serem de fácil compreensão, sobre como os dados pessoais são utilizados a partir do momento em que o uso do serviço ou da plataforma em questão é iniciado.

O que se quer dizer com 'transparência'?

Transparência significa ser claro, aberto e honesto com seus usuários sobre o que eles podem esperar quando acessam seu serviço on-line.

Por que isso é importante?

A transparência é a chave para a exigência do artigo 5(1), do RGPD, para o tratamento de dados pessoais:

O Artigo 5(1)(a), do RGPD, determina que os dados pessoais são:

> "Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência')"

O RGPD também contém disposições mais específicas sobre as informações que você deve fornecer aos titulares dos dados, quando você trata seus dados pessoais. Essas disposições são estabelecidas no artigo 13 (quando você tiver obtido os dados pessoais diretamente do titular) e no artigo 14 (quando você não tiver obtido os dados pessoais diretamente do titular).

O artigo 12, do RGPD, exige que você forneça essas informações às crianças de uma forma que elas possam acessá-las e compreendê-las:

> "O controlador tomará as medidas adequadas para fornecer ao titular de dados as informações a que se referem os artigos 13 e 14 e qualquer comunicação prevista nos artigos 15 a 22 e 34, a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas, especificamente, a crianças. As informações são prestadas por escrito ou por outros meios, inclusive, se for o caso, por meios eletrônicos. Se o titular dos dados assim solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios."

Em um nível mais amplo, a transparência também é intrínseca ao elemento de lealdade do Artigo 5(1). Se você não for claro e honesto sobre o serviço que presta e as regras que regem esse serviço, então sua coleta original e o uso contínuo dos dados pessoais da criança dificilmente serão tidos como leais.

Como podemos ter certeza de que conseguimos cumprir este padrão?

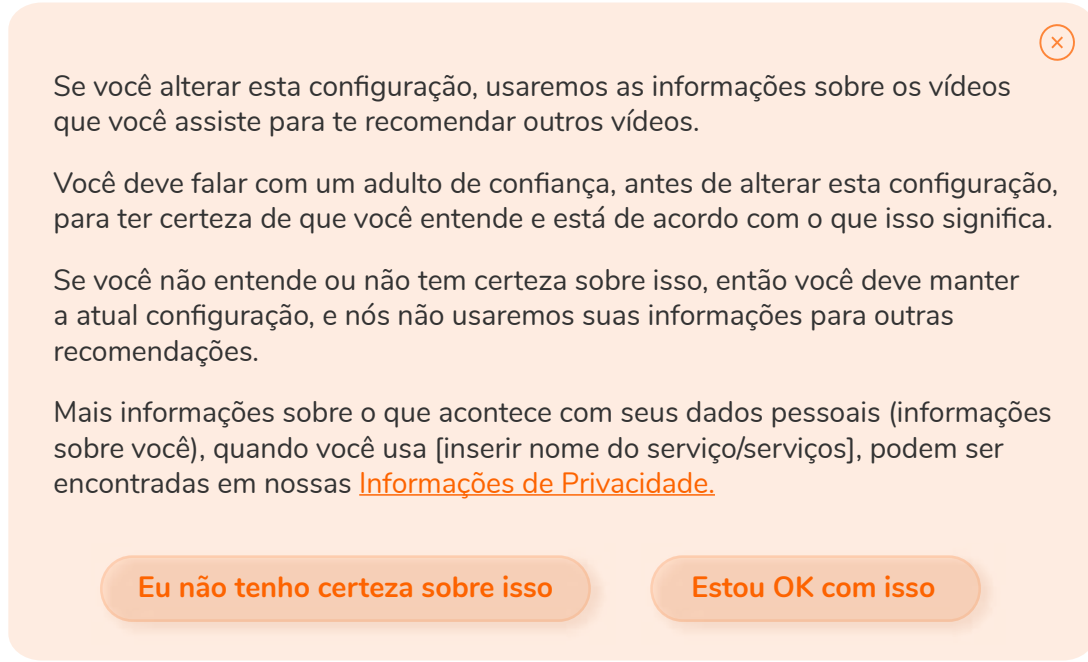
Disponibilizar informações claras sobre privacidade

Primeiro, você precisa providenciar as informações de privacidade estabelecidas nos artigos 13 e 14 em um lugar claro e proeminente em seu serviço on-line. Você deve tornar essas informações fáceis de encontrar e acessíveis para crianças e pais que buscam informações sobre privacidade.

Contudo, não é o suficiente confiar nas crianças ou em seus pais em busca dessas informações de privacidade.

Devem ser fornecidas informações em linguagem direta e acessível assim que o uso de dados pessoais for ativado.

Para proporcionar às crianças a proteção específica prevista pelo Considerando 38, você também deve providenciar informações claras sobre o que é feito com os dados pessoais em explicações mais específicas e de fácil compreensão, assim que o uso dos dados pessoais é ativado. Referem-se a esse sistema como “no momento” (*just in time*). Dependendo da idade da criança e dos riscos inerentes ao tratamento, você também deve orientá-la a falar com um adulto antes de ativar qualquer novo uso de seus dados, e não prosseguir se esses usos forem incertos.



Você também deve considerar sobre a existência de outros momentos da jornada de seu usuário que podem ser apropriados para incluir explicações adicionais específicas e de fácil compreensão, com o intuito de facilitar a compreensão da criança sobre como seus dados pessoais estão sendo usados.

Providenciar termos, políticas e padrões da comunidade claros

Todas as outras informações que você providenciar aos usuários sobre seu serviço também devem ser claras e acessíveis. Isso inclui termos e condições, políticas e padrões da comunidade.

Em todos os casos, você deve providenciar informações que sejam precisas e que não prometam proteções ou padrões que não são comuns e cumpridos de forma rotineira.

Isso deve ajudar as crianças ou seus pais a tomar decisões bem-informadas sobre se devem fornecer as informações necessárias para acessar ou assinar seu serviço, em primeiro lugar, e se devem continuar a usá-lo.

Se você acredita que precisa redigir seus termos e suas condições de forma a deixá-los juridicamente consistentes, você também pode fornecer explicações que são adequadas para a compreensão de crianças junto das explicações legais.

Apresentar informações em formato acessível às crianças (*child friendly*)

Você deve apresentar todas essas informações de forma que seja atraente e interessante à idade da criança que está acessando seu serviço on-line.

Assim, ao invés de depender somente de comunicações escritas, você pode incluir o uso de diagramas, desenhos animados, gráficos, conteúdo de vídeo e áudio, além da inclusão de plataformas de gamificação ou com conteúdo interativo que atrairá as crianças e interessar-lhes-á.

Você pode usar ferramentas como painéis de controle de privacidade, informações em camadas, ícones e símbolos para ajudar na compreensão das crianças e para apresentar as informações de uma maneira acessível para as crianças. Você deve considerar a modalidade de seu serviço e levar em conta os padrões de interação do usuário que não ocorrem em ambientes baseados em telas, conforme apropriado.

Os painéis devem ser exibidos de forma a identificar claramente e diferenciar entre o tratamento essencial para a prestação de seu serviço e o tratamento não essencial ou opcional, que a criança pode escolher se deseja ou não ativar.

Ajustar suas informações de acordo com a idade da criança

Você precisa considerar como pode personalizar o conteúdo e a apresentação das informações que você fornece, dependendo da idade do usuário.

Podem ocorrer vários cenários nos quais o fornecimento de um conjunto simplificado de informações, acessível a todos, possa funcionar. Por exemplo, se você for um varejista on-line que apenas coleta os dados pessoais necessários para concluir transações on-line e entregar mercadorias.

No entanto, em muitos casos, uma abordagem uniformizada não reconhece que as crianças têm necessidades diversas em diferentes estágios de seu desenvolvimento. Por exemplo, uma criança pré-alfabetizada ou cursando o ensino fundamental pode precisar ser ativamente impedida de mudar as configurações de privacidade sem a contribuição dos pais, enquanto um adolescente pode se basear em informações claras e neutras que o ajudem a tomar sua própria decisão informada.

Para mais informações sobre o desenvolvimento das crianças e suas necessidades, a depender de suas idades, consulte o Anexo B deste código.

Para crianças mais novas, com níveis de compreensão mais limitados, você pode precisar fornecer informações menos detalhadas para a própria criança e confiar mais no envolvimento e na compreensão dos pais. No entanto, você nunca deve usar a simplificação com o objetivo de esconder o que você está fazendo com os dados pessoais da criança. As informações devem ser providenciadas para os pais, de forma detalhada e completa, conjuntamente com as informações simplificadas e direcionadas para a criança.

Todas as versões (incluindo as versões elaboradas para os pais ou responsáveis) devem ser de fácil acesso. Além disso, é importante incorporar mecanismos que permitam que as crianças ou os pais/responsáveis possam escolher a versão visualizada, seja ela a mais complexa ou a menos complexa, a depender de seus níveis de compreensão.

Eu não entendi – você pode simplificar para mim? ↓

Está básico demais para mim – você pode me dar mais detalhes? ↑

A tabela a seguir inclui algumas recomendações. No entanto, elas são apenas um ponto de partida e você está livre para desenvolver suas próprias informações específicas de serviço e jornada do usuário (*user journey*) que levam em conta os riscos inerentes ao seu serviço.

Dependendo do tamanho de sua organização, de seu número de usuários e de sua avaliação de risco, você pode decidir realizar testes de usuários para ter certeza de que as informações fornecidas sejam suficientemente claras e acessíveis para a faixa etária em questão. Você deve documentar os resultados de qualquer teste de usuário em seu RIPD para fundamentar suas conclusões e justificar a apresentação e o conteúdo de seus recursos finais. Se você decidir que os testes com usuários não se justificam, então você deve documentar o porquê em seu RIPD.

Você também deve considerar quaisquer responsabilidades adicionais que possa ter em relação à legislação de igualdade aplicável para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

FAIXA ETÁRIA	RECOMENDAÇÕES
0-5 Pré-alfabetização e alfabetização fundamental	Providenciar informações completas e adequadas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, para os pais. Incluir avisos de áudio ou vídeo instruindo as crianças a não alterar as configurações ou a pedir ajuda a um dos pais ou a um adulto de confiança, se tentarem alterar qualquer configuração de privacidade padrão elevada.
6-9 Os principais anos do ensino fundamental	Providenciar informações completas e adequadas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, para os pais. Providenciar material de desenho animado, vídeo ou áudio junto com os recursos dos pais. Explicar os conceitos básicos de privacidade on-line dentro de seu serviço, as configurações de privacidade que você oferece, quem pode ver o quê, seus direitos de informação, e como estar no controle de suas próprias informações e respeitar a privacidade de outras pessoas. Explicar os conceitos básicos de seu serviço e como ele funciona, o que eles podem esperar de você e o que você espera deles. Oferecer recursos para que os pais possam usar com seus filhos, no sentido de explicar os conceitos de privacidade e os riscos dentro do serviço em questão. Os recursos disponíveis para os pais devem ser adequados, a fim de que eles consigam explicar para os filhos como o serviço funciona, o que eles podem esperar de você e o que você espera deles. Se uma criança tentar alterar uma configuração padrão de privacidade elevada, forneça materiais de desenho animado, vídeo ou áudio para explicar o que acontecerá com suas informações e quaisquer outros riscos associados. Diga a elas para deixar as coisas como estão ou pedir ajuda aos pais ou a um adulto de confiança antes de alterar a configuração. Providenciar informações completas e adequadas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, para os pais. Fornecer informações completas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, em um formato adequado para crianças dentro desta faixa etária. Permitir que as crianças escolham entre opções escritas e opções de vídeo/áudio. Dar às crianças a opção de ampliar ou de reduzir as informações que elas veem (para materiais desenvolvidos para uma faixa etária maior ou menor), dependendo de suas necessidades individuais. Se uma criança tentar alterar uma configuração padrão de privacidade elevada, forneça materiais de desenho animado, vídeo ou áudio para explicar o que acontecerá com suas informações e quaisquer outros riscos associados. Diga a elas para deixar as coisas como estão ou pedir ajuda aos pais ou a um adulto de confiança antes de alterar a configuração.

10-12 Anos de transição escolar	Providenciar informações completas e adequadas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, para os pais. Fornecer informações completas sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, em um formato adequado para crianças dentro desta faixa etária. Permitir que as crianças escolham entre opções escritas e opções de vídeo/áudio. Dar às crianças a opção de ampliar ou de reduzir as informações que elas veem (para materiais desenvolvidos para uma faixa etária maior ou menor), dependendo de suas necessidades individuais. Se uma criança tentar alterar uma configuração padrão de privacidade elevada, forneça materiais de desenho animado, vídeo ou áudio para explicar o que acontecerá com suas informações e quaisquer outros riscos associados. Diga a elas para deixar as coisas como estão ou pedir ajuda aos pais ou a um adulto de confiança antes de alterar a configuração.
13-15 Início da adolescência	Providenciar informações sobre privacidade, conforme exigido pelos artigos 13 & 14, do RGPD, em um formato adequado para esta faixa etária. Permitir que eles escolham entre opções escritas e opções de vídeo/áudio. Dê a eles a opção de ampliar ou de reduzir as informações disponibilizadas (quanto a materiais desenvolvidos para uma faixa etária maior ou menor), dependendo de suas necessidades individuais. Se ocorrer a tentativa de alterar uma configuração padrão de privacidade elevada, forneça materiais por escrito, vídeo ou áudio para explicar o que acontecerá com suas informações e quaisquer outros riscos associados. Incentive que eles procurem ajuda dos pais ou de um adulto de confiança antes de alterar a configuração, se tiverem alguma dúvida/preocupação ou se não compreenderem as informações dadas. Fornecer informações completas em um formato adequado para os pais, em conjunto com a informação disponibilizada para a faixa etária em questão.
16-17 Aproximando-se da maioridade	Providenciar informações completas em um formato adequado para esta faixa etária. Permitir que eles escolham entre opções de explicações por escrito ou por meio de vídeo/áudio. Dar a eles a opção de ampliar ou de reduzir as informações disponibilizadas (quanto a materiais desenvolvidos para uma faixa etária maior ou menor), dependendo de suas necessidades individuais. Se ocorrer a tentativa de alterar uma configuração padrão de privacidade elevada, forneça materiais por escrito, vídeo ou áudio para explicar o que acontecerá com suas informações e quaisquer outros riscos associados. Incentive que eles confirmem com um adulto ou com outra fonte de informação segura e que não alterem as configurações, se tiverem alguma dúvida/preocupação ou se não compreenderem as informações dadas. Fornecer informações completas em um formato adequado para os pais, em conjunto com a informação disponibilizada para a faixa etária em questão.

Para mais informações além deste código:

Guia para o RGPD - licitude, lealdade e transparência

Guia para o RGPD - o direito de ser informado

5. USO INDEVIDO DE DADOS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Não utilizar dados pessoais de crianças para fins que se mostraram prejudiciais ao seu bem-estar, ou que vão contra códigos de prática da indústria, outras disposições regulatórias ou conselhos do governo.

O que se quer dizer com 'uso indevido de dados'?

'Uso indevido de dados' refere-se a qualquer uso de dados que seja obviamente prejudicial à saúde física ou mental e ao bem-estar de crianças ou que vá contra códigos de prática da indústria, outras disposições regulatórias ou orientações do governo sobre o bem-estar das crianças.

Por que isso é importante?

O artigo 5(1)(a), do RGPD, estabelece que os dados pessoais devem ser tratados de forma lícita, leal e transparente, em relação ao titular de dados, e o Considerando 38 determina que as crianças merecem proteção específica, no que diz respeito ao uso de seus dados pessoais.

O Considerando 2 ao RGPD assegura que:

> 2) "Os princípios e as regras em matéria de proteção de pessoas naturais, relativamente ao tratamento de seus dados pessoais, deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e as suas liberdades fundamentais, nomeadamente, o direito à proteção de dados pessoais. ***O presente regulamento tem como objetivo contribuir para (...) o bem-estar de pessoas físicas."***

O Considerando 75 ao RGPD determina que:

> "O risco para os direitos e as liberdades de pessoas naturais, ou a probabilidade e a gravidade de riscos variáveis, pode resultar do tratamento de dados pessoais capazes de levar a danos físicos, materiais ou não materiais, sobretudo (....), onde os dados pessoais de pessoas naturais vulneráveis, em particular, crianças, são tratados...".

Significa dizer que você não deve tratar dados pessoais de crianças de formas que sejam obviamente – ou tenham sido, comprovadamente, – prejudiciais à saúde ou ao bem-estar delas. Fazer isso não seria leal.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Mantenha-se sempre atualizado com recomendações e orientações relevantes

Como provedor de um serviço on-line que, provavelmente, será acessado por crianças, você deve estar ciente das normas e dos códigos de prática relevantes dentro de sua indústria ou seu setor, e de qualquer disposição contida neles que se relacione a crianças. Você também deve se manter atualizado com as orientações do governo sobre o bem-estar de crianças, no contexto de serviços digitais ou on-line. A ICO não regulamenta o conteúdo e não é especialista em questões de saúde e bem-estar das crianças. No entanto, nos referiremos a outros códigos de prática ou a outras orientações regulatórias, quando relevantes, para nos ajudar a avaliar sua conformidade com este padrão.

Não tratar os dados pessoais de crianças de forma que seja obviamente indevida e prejudicial ou contrária a estes conselhos

Você não deve tratar os dados pessoais de crianças de maneira contrária a estes parâmetros, códigos, orientações ou conselhos e deve levar em conta qualquer orientação específica de idade para adequar seu serviço on-line à idade da criança. Atenção ao fazer o perfilamento de crianças, assim como fazer inferências baseadas em seus dados pessoais ou tratar dados de geolocalização.

Você deve seguir uma abordagem de precaução nos casos em que isso tenha sido formalmente recomendado, apesar de as provas estarem ainda em discussão. Isso significa que o tratamento de dados pessoais de crianças não deve ser feito, se já existirem provas formais de que há necessidade e exigência de mais pesquisas ou provas para estabelecer se o tratamento é ou não prejudicial ou indevido à saúde e ao bem-estar das crianças.

Quais códigos ou conselhos podem ser relevantes?

Algumas áreas específicas, nas quais há orientação relevante, e que provavelmente surgirão no contexto da prestação de seu serviço on-line, são apresentadas a seguir.

No entanto, esta não é uma lista exaustiva e você precisa identificar e considerar tudo que for relevante para seu cenário específico de tratamento de dados em seu RIPD.

Marketing e publicidade comportamental

O Comitê de Práticas Publicitárias (CAP, sigla em inglês) publica orientações sobre publicidade comportamental on-line que, além de fornecer regras aplicáveis a toda publicidade, cobre, especificamente, a publicidade para crianças.

- Algumas regras do CAP abordam questões como:
- danos físicos, mentais ou morais às crianças;
- exploração da credulidade das crianças e aplicação de pressões injustas;
- exortação direta às crianças e debilitamento da autoridade dos pais; e
- promoções.

Também dispõe de regras que disciplinam ou proíbem a comercialização de certos produtos, como alimentos e bebidas com alto teor de gordura, sal, açúcar e álcool, para crianças, e de orientações gerais sobre transparência de conteúdo pago e colocação de produtos.

Veiculação

A agência Ofcom publicou um código de práticas para emissoras, que abrange a proteção de menores de 18 anos nas seguintes áreas:

- crimes sexuais e outros, no Reino Unido, envolvendo menores de 18 anos;
- drogas, tabagismo, solventes e álcool;
- violência e comportamentos perigosos;
- linguagem ofensiva;
- material sexual;
- nudez;
- exorcismo, ocultismo e o paranormal;
- e envolvimento de pessoas com menos de 18 anos em programas.

A imprensa

A *Independent Press Standards Organization* (IPSO)[14] publicou O Código de Prática dos Editores (*The Editors' Code of Practice*), que inclui disposições sobre reportagens e crianças.

---

14. A *Independent Press Standards Organization* é o maior regulador independente da indústria de jornais e revistas do Reino Unido. Disponível em: <https://www.ipso.co.uk/>. Acesso em 26 de maio de 2021.

Jogos on-line

O Gabinete de Comércio Justo (OFT, na sigla em inglês) publicou princípios que devem ser aplicados em jogos on-line e em jogos de aplicativos, que incluem disposições sobre:

- a exploração da inexperiência, da vulnerabilidade e da credulidade das crianças, inclusive através de práticas comerciais agressivas; e
- a inclusão de exortações diretas às crianças para que comprem produtos anunciados ou convençam seus pais ou outros adultos a comprar produtos anunciados para elas.

Estratégias utilizadas para ampliar o engajamento dos usuários

Estratégias usadas para estender o engajamento do usuário, às vezes referidas como *sticky features*, podem incluir mecanismos como *reward loops*, *continuous scrolling,* notificações e recursos de reprodução automática que incentivam os usuários a continuar jogando, assistindo a vídeos ou permanecendo on-line de alguma forma.

Apesar de não haver, atualmente, um posicionamento formal do governo acerca do efeito desses mecanismos sobre a saúde e o bem-estar das crianças, os Oficiais Médicos Chefes (OFC) do Reino Unido emitiram um 'comentário sobre exposição de crianças e jovens a atividades em tela'. Este identifica a necessidade de mais pesquisa e recomenda que as empresas de tecnologia 'apliquem uma abordagem preventiva no desenvolvimento de estruturas e removam as ferramentas viciantes'.

Isso significa que não podemos usar recursos como recompensas, notificações e 'curtidas' dentro de nosso serviço?

Não, nem todos os recursos dependem do uso de dados pessoais. Além disso, você pode ter feito o *design* de seu recurso levando em consideração as necessidades das crianças e de uma forma que seja fácil de elas cessarem o engajamento, sem se sentirem pressionadas ou prejudicadas de alguma forma. Isso significa, no entanto, que você precisa considerar cuidadosamente o impacto sobre as crianças, se você usar seus dados pessoais para justificar esses recursos. Você deve considerar as consequências intencionais e não intencionais do uso dos dados como parte de seu RIPD.

Considerando as recomendações de CMOs acerca de uma abordagem precaucionária, o desenvolvimento de recursos baseados em dados que dificultem o desengajamento de crianças com o serviço, provavelmente, violará o Artigo 5 (1)(a), do RGPD, que prevê o tratamento de

dados de forma leal. Por exemplo, recursos que usam dados pessoais para explorar a suscetibilidade humana a recompensas, a comportamentos antecipatórios e que visam ao prazer ou à pressão social.

Você deve:

- evitar o uso de dados pessoais de forma a incentivar as crianças a permanecer engajadas através, por exemplo, de vantagens personalizadas embutidas em jogos (apoiado no uso individual de seus dados pessoais), em troca de tempo prolongado no jogo/partida
- apresentar opções para continuar jogando ou se engajando de outra forma com o seu serviço, de forma neutra, sem sugerir que as crianças seriam prejudicadas em caso contrário;
- evitar recursos que utilizem dados pessoais para estender o tempo de tela, automaticamente, do usuário, em vez de exigir que as crianças façam uma escolha ativa sobre se querem gastar seu tempo dessa forma (recursos de reprodução automática baseados em dados);
- introduzir mecanismos de pausa que permitam que as crianças façam uma pausa a qualquer momento, sem perder o progresso em um jogo, ou fornecer conteúdo apropriado para a idade, a fim de apoiar escolhas conscientes sobre fazer um intervalo, como as fornecidas nas orientações providenciadas pelos CMOs.

Para leituras além deste código:

- Guia do Comitê de Prática Publicitária (CAP)
- The Ofcom Broadcasting Code (with the Cross-promotion Code and the On Demand Program Service Rules)
- Código de Práticas dos Editores
- Os princípios para jogos e aplicativos on-line do Gabinete de Comércio Justo (OFT)
- United Kingdom Chief Medical Officers' commentary on 'Screen--based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'

6. POLÍTICAS E PADRÕES DA COMUNIDADE *(COMMUNITY STANDARDS)*

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Sustentar seus próprios termos publicados, suas próprias políticas e seus próprios padrões da comunidade (incluindo, mas não limitados a, políticas de privacidade, restrição de idade, regras de comportamento e políticas de conteúdo).

O que se quer dizer com 'manter os seus próprios padrões'?

Queremos dizer que você precisa aderir aos seus próprios termos e condições publicados e às suas próprias políticas.

Significa que, quando você estabelece regras e condições de uso da comunidade para os usuários de seu serviço, você precisa aplicar e cumprir ativamente essas regras e condições.

Por que isso é importante?

O Artigo 5(1), do RGPD, determina que os dados pessoais serão:

> Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência').

Quando crianças fornecem seus dados pessoais a fim de aderir ou acessar seu serviço, elas devem ser capazes de esperar que o serviço funcione adequadamente, conforme lhes foi prometido. Se isso não acontecer, a coleta dos dados pessoais pode ser injusta e violar o Artigo 5(1)(a).

Sustentar e manter seus próprios padrões também deve beneficiá-lo, dando às crianças e aos pais a segurança de que podem confiar no seu serviço on-line com seus dados pessoais.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Até certo ponto, isso depende do conteúdo de seus termos e condições publicados, políticas e padrões da comunidade.

No entanto, você deve respeitar o princípio fundamental de "você diz o que faz e faz o que diz". Você deve ao menos assegurar que:

Só utilize dados pessoais de acordo com sua política de privacidade

O Artigo 5(1)(b), do RGPD, prevê o 'princípio da limitação da finalidade', segundo o qual os dados pessoais serão:

> "recolhidos para finalidades determinadas, explícitas e legítimas não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades..."

Os artigos 13 e 14, do RGPD exigem que você informe aos titulares dos dados quais são essas finalidades. Isso é feito, fornecendo informações de privacidade, que você pode incluir em notificação, política ou declaração de privacidade.

O artigo 5(1)(a), do RGPD, exige que você trate os dados pessoais de forma leal e transparente.

O resultado obtido com essas disposições é que você precisa usar suas informações de privacidade para informar aos usuários o que será feito com seus dados pessoais e por que, e então se certificar de que você siga isso na prática.

Cumprir com as políticas de comportamento do usuário

Se você tem alguma regra publicada que regula o comportamento dos usuários de seu serviço, então você precisa cumprir e seguir essas regras e colocar em prática os sistemas que você disse que iria cumprir. Portanto, se você diz que monitora ativamente o comportamento dos usuários, ou oferece moderação em tempo real, automatizada ou humana das funções de 'chat', então você precisa fazer isso.

Se você só depende de processos '*back end*'[15], como relatórios de usuários, para identificar comportamentos que violam suas políticas, então você precisa ter deixado isso bem claro em suas políticas ou padrões da comunidade. Essa abordagem também precisa ser razoável, dados os riscos para crianças de diferentes idades inerentes ao seu serviço. Se os riscos forem altos, então os processos de '*light touch*'[16] ou '*back end*' dificilmente serão suficientes para cumprir com os seus padrões.

---

15. "Back-end é toda a parte da programação voltada ao funcionamento interno de um software. Em outras palavras, back-end é tudo aquilo que está por trás da interface de uma aplicação: seus sistemas, seu banco de dados, toda a parte de segurança de dados, envio e recebimento de informações, armazenamento etc.". Disponível em: <https://kenzie.com.br/blog/back-end/>. Acesso em 15 de abril de 2021.

16. "Definido pelo baixo nível de interação humana entre potenciais clientes e representantes comerciais durante todo o funil de vendas.". Disponível em: <https://startupi.com.br/>. Acesso em 15 de abril de 2021.

Se você não tiver sistemas adequados para sustentar adequadamente suas próprias políticas de comportamento do usuário, então sua coleta original e o uso contínuo dos dados pessoais de uma criança pode ser injusta, isto é, de forma não leal, violando o RGPD.

Cumprir com o prometido em relação a conteúdo e outras políticas

Se você se comprometer com os usuários sobre o conteúdo ou os outros aspectos de seu serviço on-line, então você precisa ter sistemas para assegurar que você cumpra com esses compromissos.

Portanto, se você afirmar que o conteúdo de seu serviço on-line é adequado para crianças dentro de uma determinada faixa etária, então você precisa ter sistemas para assegurar que ele realmente seja adequado. Se você disser que não tolera *bullying*, então você precisa ter mecanismos adequados para lidar rápida e efetivamente com incidentes de *bullying*.

Novamente, se seus sistemas não forem adequados ou se você não cumprir suas promessas, então sua coleta original e o uso continuado dos dados pessoais da criança podem ser considerados como não leais ou injustos e violar o RGPD.

Se você tem políticas diferentes dependendo da idade de seus usuários, então você precisa levar em conta a idade da criança ao defender suas políticas.

7. CONFIGURAÇÕES PADRÃO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

As configurações devem ser 'alta privacidade' por padrão (a menos que você possa demonstrar uma razão convincente para uma configuração padrão diferente, levando em conta o melhor interesse da criança).

O que se quer dizer com 'configuração de privacidade por padrão'?

As configurações de privacidade são uma forma prática de oferecer às crianças uma escolha sobre como seus dados pessoais são usados e protegidos. Você pode usá-las sempre que coletar e tratar dados pessoais das crianças, a fim de 'melhorar' ou 'personalizar' sua experiência on-line, além da prestação de seu serviço principal.

As configurações incluem a forma como os dados pessoais das crianças são utilizados:

- em um sentido interpessoal; à medida em que os dados pessoais se tornam visíveis ou acessíveis a outros usuários de seu serviço on-line;
- por você mesmo, como provedor do serviço on-line; por exemplo, usando dados pessoais para sugerir compras dentro do app; e
- por terceiros; por exemplo, para permitir que terceiros promovam ou comercializem produtos.

As configurações padrão de privacidade administram o uso dos dados pessoais das crianças se elas não realizarem alterações nas configurações, quando começarem a usar seu serviço on-line.

Por que elas são importantes?

Muitas crianças simplesmente aceitarão qualquer configuração padrão que você fornecer e nunca mudarão suas configurações de privacidade. Isso significa que é de extrema importância que as configurações padrão que você definir sejam adequadas para as crianças e lhes forneçam proteção adequada, na forma como seus dados pessoais são utilizados. Para crianças, não é suficiente permitir que elas ativem configurações de alta privacidade; você precisa fornecê-las por padrão (a menos que tenha uma razão convincente para fazer o contrário, levando em conta o melhor interesse da criança).

Também são importantes, devido ao artigo 25(2), do RGPD:

> "25(2) O controlador responsável pelo tratamento aplicará medidas técnicas e organizacionais adequadas para assegurar que, por padrão, somente os dados pessoais necessários para cada finalidade específica do tratamento sejam tratados. Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão de seu tratamento, ao período de armazenamento e à sua acessibilidade. Essas medidas devem assegurar que, por padrão, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas físicas, sem a intervenção do indivíduo."

Isto significa que, por padrão, você não deve:

- coletar mais dados pessoais do que os necessários para providenciar cada elemento individual de seu serviço on-line; ou
- tornar os dados pessoais de seus usuários visíveis a um número indefinido de outros usuários de seu serviço on-line.

Você também pode usar configurações de privacidade para ajudar no exercício dos direitos de proteção de dados de crianças (como o direito de se opor ao tratamento ou de restringi-lo). Ao implementar essas configurações, você pode proporcionar às crianças e aos pais maior confiança em suas interações com seu serviço on-line e ajudá-los a explorar as implicações de permitir que você use os dados pessoais de diferentes formas.

É necessário providenciar uma configuração de privacidade toda vez que usamos os dados pessoais de uma criança?

Sempre que for possível, você deve fornecer configurações de privacidade (definidas como alta privacidade por padrão) para dar às crianças controle sobre quando e como você usa seus dados pessoais.

Não é necessário que você forneça uma configuração de privacidade para qualquer dado pessoal que você tenha que tratar, a fim de fornecer seu serviço principal ou o mais básico. Isso porque, sem esse tratamento essencial, não há nenhum serviço básico para você oferecer. Nessa circunstância, se a criança desejar acessar o serviço principal, você não poderá oferecer a ela uma escolha sobre se seus dados pessoais serão processados ou não.

Com o intuito de dar às crianças controle sobre quando e como seus dados pessoais são usados, você deve oferecer configurações de privacidade para qualquer tratamento que seja necessário, no sentido de fornecer recursos adicionais de serviço que vão além do serviço principal.

Examinaremos com muito cuidado qualquer reivindicação de que um ambiente de privacidade não pode ser fornecido, porque os dados pessoais são necessários para fornecer o serviço principal. Em relação a isso, você deve seguir, não apenas a literalidade, mas também o espírito do código, ou seja, sua intenção, bem como tomar cuidado para não abusar do conceito de um serviço principal e aplicá-lo de forma mais ampla do que é esperado e necessário.

Veja também o Anexo C deste código 'Bases legais para tratamento', que explica a necessidade de diferenciar elementos centrais e não centrais de seu serviço, em qualquer caso, a fim de identificar uma base legal apropriada para o tratamento, conforme exigido pelo RGPD.

Também podem haver alguns outros tipos limitados de tratamento, em relação aos quais não é adequado oferecer um ambiente de privacidade. Por exemplo, se você precisar tratar os dados pessoais de uma criança, a fim de cumprir uma obrigação legal (como uma exigência de proteção à criança) ou para prevenir a exploração e o abuso sexual infantil on-line. Não é então adequado oferecer a eles uma escolha sobre se seus dados pessoais são tratados para esse fim ou não.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Proporcionar configurações 'alta privacidade' por padrão

Se for o caso de oferecer uma configuração de privacidade, então você deve definir cada configuração individual como sendo de 'alta privacidade' por padrão.

Isso significa que os dados pessoais de crianças só são visíveis ou acessíveis aos outros usuários do serviço, se a criança alterar suas configurações para permitir isso.

Isso também significa que, a menos que a configuração seja alterada, seu uso dos dados pessoais de crianças é limitado ao uso que é essencial para a prestação do serviço. Quaisquer usos opcionais dos dados pessoais, incluindo quaisquer usos projetados para personalizar o serviço, devem ser selecionados individualmente e ativados pela criança.

Da mesma forma, qualquer configuração a qual permita que terceiros utilizem dados pessoais deve ser ativada pela criança.

A exceção a essa regra é se você puder demonstrar que existe uma razão convincente para uma configuração padrão diferente, considerando o melhor interesse da criança.

Considerar a necessidade de maiores intervenções no momento em que qualquer configuração for alterada

Ao definir que as configurações de alta privacidade por padrão, por si só, mitigam os riscos para crianças, uma vez que, na maioria das vezes, essas configurações de privacidade por padrão nunca serão alteradas.

Da mesma forma, providenciar explicações e avisos adequados à idade, quando uma criança tenta mudar uma configuração de privacidade, conforme exigido pelo padrão de transparência, também mitigará o risco.

No entanto, você também deve considerar se deve colocar em prática outras medidas, quando uma criança tenta alterar uma configuração. Isso depende de sua avaliação dos riscos inerentes ao tratamento envolvido em cada configuração e poderia incluir outras medidas de controle de idade. Você deve usar seu RIPD para ajudá-lo a avaliar os riscos e a identificar a mitigação adequada.

Permitir aos usuários a opção de alterar as configurações permanentemente ou apenas para o uso atual

Se um usuário alterar suas configurações, você deve oferecer-lhe a opção de fazê-lo permanentemente ou retornar aos altos padrões de privacidade, quando terminar a sessão atual. Você não deve utilizar técnicas *nudge* para que optem por uma opção de privacidade mais baixa (para mais informações sobre isso, consulte a seção deste código sobre técnicas de *nudge*). No que tange aos dados de geolocalização, considerações ligeiramente diferentes se aplicam, uma vez que tornam a localização da criança visível aos outros. Isso é tratado com mais detalhes na seção deste código sobre geolocalização.

Em síntese, você precisa demonstrar que facilitou a manutenção ou o retorno às configurações de alta privacidade para uma criança, se ela assim desejar.

Preserve as escolhas do usuário ou os altos padrões de privacidade, quando o software for atualizado

Se você introduzir uma atualização de software (por exemplo, para atualizar medidas de segurança ou introduzir novos recursos), então você deverá manter quaisquer configurações de privacidade que o usuário tenha aplicado. Se não for possível fazer isso (por exemplo, se um novo aspecto ou um novo recurso do produto ou serviço for introduzido, ou se um recurso existente for alterado significativamente, de modo que as configurações de privacidade anteriores não sejam mais relevantes), você deve definir a nova configuração como alta privacidade por padrão.

Permitir escolhas diferentes para o usuário em dispositivos de multiusuários

Se você providencia um serviço on-line que permite que vários usuários acessem o serviço a partir de um único dispositivo, então, sempre que possível, você deve permitir que os usuários configurem seus próprios perfis, com suas próprias configurações individuais de privacidade. Isso significa que as crianças não precisam compartilhar as configurações de privacidade de um adulto, quando compartilham o mesmo dispositivo. Os perfis podem ser acessados através de opções baseadas na tela, ou usando-se a tecnologia de reconhecimento de voz para serviços on-line ativados por voz.

Você deve incluir informações inequívocas para a pessoa que configura ou registra o dispositivo, alertando-a sobre o potencial de coleta de dados pessoais de múltiplos usuários.

As configurações de privacidade são um mecanismo de consentimento?

Para que o consentimento seja válido em relação ao RGPD, ele precisa atender à seguinte definição:

> RGPD Artigo 4(11)
>
> "'Consentimento' do titular dos dados significa qualquer manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"

Se suas configurações estiverem desativadas por padrão e o usuário tiver que ativar o tratamento, alterando a configuração padrão, então você poderá usar as configurações de privacidade como parte de seu mecanismo para obter o consentimento de seu tratamento em relação ao RGPD. Entretanto, você também precisa cumprir os requisitos do artigo 7 (condições para consentimento), do RGPD, e os requisitos de verificação de idade e responsabilidade parental do artigo 8 (os quais só permitem que crianças de 13 anos ou mais forneçam seu próprio consentimento), de modo que não serão suficientes por si só.

As configurações de privacidade não são relevantes apenas para o consentimento. Você também pode usá-las para dar às crianças a escolha sobre como seus dados pessoais serão usados, se você confiar em outras bases legais para o tratamento (como interesses legítimos) que não tenham nenhuma exigência formal de consentimento.

Para mais informações sobre bases legais para o tratamento de dados, incluindo consentimento, consulte as orientações complementares no Anexo C. Você também pode querer consultar o seu DPO, caso tenha um.

8. MINIMIZAÇÃO DE DADOS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> O mínimo de dados pessoais deve ser coletado e retido para que sejam fornecidos os recursos de seu serviço, nos quais uma criança está ativa e conscientemente envolvida. Dê às crianças escolhas separadas sobre os recursos que elas desejam ativar.

O que se quer dizer com 'minimização de dados'?

A minimização de dados significa a coleta de uma quantidade mínima de dados pessoais que você precisa para fornecer um recurso individual de seu serviço. Isso significa que você não pode coletar mais dados do que os necessários para fornecer os recursos de um serviço que a criança realmente deseja utilizar.

Por que isso é importante?

O artigo 5(1)(c), do RGPD, estabelece que os dados pessoais devem ser:

> "adequados, relevantes e limitados ao que é necessário, relativamente às finalidades para as quais são tratados ('minimização de dados');

O artigo 25, do RGPD, prevê que esta abordagem deve ser aplicada por padrão a 'cada finalidade específica do tratamento'.

Ele se alinha ao princípio de 'limitação da finalidade' estabelecido no artigo 5(1)(b), do RGPD, que estabelece que a finalidade para a qual você coleta dados pessoais deve ser 'específica, explícita e legítima' e ao princípio de limitação de armazenamento estabelecido no artigo 5(1)(e), o qual estabelece que os dados pessoais devem ser mantidos 'não mais do que o necessário', em relação às finalidades para as quais são tratados.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Identificar quais dados pessoais você precisa para fornecer cada recurso individual de seu serviço

O RGPD exige que você seja claro quanto às finalidades para as quais você coleta dados pessoais, que somente colete a quantidade

mínima de dados pessoais necessários para essas finalidades e que somente armazene esses dados durante o mínimo de tempo que você precisar. Isso significa que você precisa diferenciar cada elemento individual de seu serviço e considerar quais dados pessoais você precisa, e por quanto tempo, para entregar cada um dos serviços.

Exemplo:

Você oferece um serviço de download de música.

Um recurso de seu serviço é permitir que os usuários procurem faixas que talvez queiram baixar.

Outro recurso pode ser o de fazer recomendações aos usuários com base em buscas anteriores, escuta e downloads.

Um outro recurso é compartilhar o que os usuários individuais estão escutando com outros grupos de usuários.

Todos esses são recursos separados de seu serviço global. Os dados pessoais que você precisa fornecer para cada recurso variam.

Dê às crianças a escolha sobre quais recursos de seu serviço elas desejam usar

Você deve proporcionar às crianças o máximo de escolhas possíveis sobre quais recursos de seu serviço elas desejam utilizar e, portanto, quantos dados pessoais elas precisam fornecer.

Isso é particularmente importante para sua coleta de dados pessoais, a fim de ‘melhorar’, ‘aprimorar’ ou ‘personalizar’ a experiência on-line de seus usuários, além da prestação de seu serviço principal.

Você não deve ‘agrupar’ sua coleta de dados pessoais de crianças, para fornecer essas melhorias, com a coleta de dados pessoais que você precisa para fornecer o serviço principal, pois você está efetivamente coletando dados pessoais para diferentes propósitos ou finalidades. Você também não deve agrupar vários elementos adicionais ou aprimoramentos do serviço. Você deve proporcionar às crianças uma escolha se desejam que seus dados pessoais sejam usados para cada finalidade adicional ou aprimoramento do serviço. Você pode fazer isso através de suas configurações de privacidade padrão, conforme abordado na seção anterior deste código.

Somente colete dados pessoais, quando a criança estiver usando ativa e conscientemente esse recurso do seu serviço

Você só deve coletar os dados pessoais necessários para fornecer cada recurso de seu serviço, quando a criança estiver ativa e conscientemente envolvida com esse elemento do serviço.

Exemplo:

É aceitável coletar a localização de uma criança, quando ela estiver usando um recurso de seu serviço baseado em mapas, com o intuito de ajudá-la a encontrar o caminho para um destino específico, e se você providenciar um sinal óbvio a fim de que ela saiba que sua localização está sendo rastreada.

Não é aceitável continuar a rastrear sua localização após terem fechado o mapa ou chegado ao seu destino.

Para leituras além deste código:

Guia para o RGPD - minimização de dados

9. COMPARTILHAMENTO DE DADOS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Não divulgar os dados das crianças, a menos que você possa demonstrar uma razão convincente para fazê-lo, levando em conta o melhor interesse da criança.

O que se quer dizer com 'compartilhamento de dados'?

Compartilhar dados, geralmente, significa revelar dados pessoais a terceiros fora de sua organização. Também pode abranger o compartilhamento de dados pessoais entre diferentes partes de sua própria organização ou outras organizações dentro do mesmo grupo ou sob a mesma empresa matriz.

O compartilhamento de dados pode ser feito rotineiramente (por exemplo, o provedor de um aplicativo educacional compartilhando, rotineiramente, dados com a escola da criança) ou em resposta a uma situação única ou emergencial (por exemplo, compartilhando os dados pessoais da criança com a polícia por razões de proteção).

O compartilhamento de dados inclui tornar os dados pessoais de uma criança visíveis para terceiros.

Por que isso é importante?

É importante, porque, se você compartilhar os dados pessoais de crianças com terceiros ou com outras partes de sua própria organização, é necessário que fazer isso seja leal para com a criança. O compartilhamento de dados pessoais de crianças com terceiros, incluindo o compartilhamento de dados inferidos ou derivados de seus dados pessoais, pode expor as crianças a riscos decorrentes de seu tratamento de dados pessoais, que vão além daqueles inerentes ao seu próprio tratamento.

O RGPD estabelece que:

> "5(1) Dados pessoais são:
>
> (a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
>
> (b) Coletados para finalidades específicas, explícitas e legítimas e não podendo ser processados, posteriormente, de uma forma incompatível com essas finalidades".

Os artigos 13 e 14, do RGPD, exigem que você informe aos titulares com quem você compartilha os dados pessoais (os destinatários ou as categorias de destinatários dos dados pessoais).

Como podemos ter certeza de que conseguimos cumprir este padrão?

Considerar o melhor interesse da criança

O melhor interesse da criança deve ser uma consideração primordial sempre que você considerar compartilhar os dados pessoais de crianças.

Se você já se certificou de que suas configurações de privacidade estão definidas como 'alta privacidade' por padrão, então a quantidade de compartilhamento de dados que ocorre já deve ser limitada; com as crianças tendo que alterar ativamente as configurações padrão, para permitir que você compartilhe seus dados pessoais em muitas circunstâncias.

Você não deve compartilhar dados pessoais, se você puder prever, razoavelmente, que isso resultará na utilização de dados pessoais de crianças por terceiros de maneiras que se demonstram prejudiciais ao seu bem-estar. Você deve obter garantias de quem quer que compartilhe os dados pessoais sobre isso e realizar as devidas verificações de diligência quanto à adequação de suas práticas de proteção de dados e qualquer distribuição posterior dos dados.

Qualquer configuração padrão relacionada ao compartilhamento de dados deve especificar a finalidade do compartilhamento e com quem os dados serão compartilhados. As configurações que permitam o compartilhamento geral ou ilimitado não serão compatíveis ou aceitas.

Em última análise, cabe à pessoa com quem você compartilhou os dados garantir que eles cumpram os requisitos do RGPD (em seu papel de controlador de dados para os dados pessoais que eles recebem). Contudo, você é responsável por assegurar que o compartilhamento de dados pessoais cumpra com o requisito de lealdade em primeiro lugar. Você não deve compartilhar os dados pessoais, a menos que tenha uma razão convincente para fazê-lo, levando em conta o melhor interesse da criança.

Um exemplo claro de uma razão convincente é o compartilhamento de dados para fins de proteção, prevenção da exploração e abuso sexual infantil on-line, ou para fins de prevenção ou detecção de crimes contra crianças, como o aliciamento on-line.

Um exemplo que dificilmente será uma razão convincente para o compartilhamento de dados é a venda de dados pessoais de crianças para reutilização comercial.

Considere as questões e os riscos específicos levantados em cada etapa de seu RIPD

Você deve avaliar os problemas e os riscos levantados em cada etapa individual de seu RIPD. Essas etapas estão definidas e explicadas na seção deste código sobre RIPDs.

Para leituras além deste código:

Para leitura adicional sobre compartilhamento de dados, veja nosso Código de Prática de Compartilhamento de Dados.

10. GEOLOCALIZAÇÃO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Desativar as opções de geolocalização por padrão (a menos que você possa demonstrar uma razão convincente para que a geolocalização esteja ativada por padrão, levando em conta o melhor interesse da criança). Providenciar um aviso óbvio para crianças, quando o rastreamento de localização estiver ativo. As opções que tornam a localização de uma criança visível para os outros devem ser desativadas por padrão ao final de cada sessão.

O que se quer dizer com 'dados de geolocalização'?

Dados de geolocalização significam dados retirados de um dispositivo do usuário que indicam a localização geográfica desse dispositivo, incluindo dados de GPS ou dados sobre conexão com equipamento wi-fi local.

Por que isso é importante?

O Considerando 38, do RGPD, determina que:

> "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais...."

O uso de dados de geolocalização, em relação às crianças, é de especial preocupação. Isso porque a capacidade de verificar ou rastrear a localização física de uma criança traz consigo o risco de que os dados possam ser mal utilizados para comprometer a segurança física dessa criança. Em resumo, pode tornar as crianças vulneráveis a riscos como sequestro, abuso físico e mental, abuso sexual e tráfico.

O compartilhamento persistente da localização também pode significar que as crianças têm um senso diminuído de seu próprio espaço privado, o que pode afetar o desenvolvimento de seu senso em relação à própria identidade. Pode, potencialmente, não respeitar os direitos da criança tutelados pela CNUDC, em relação à privacidade, à liberdade de associação e à liberdade de exploração econômica, independentemente de ameaças à sua segurança física.

Todos os serviços de geolocalização devem ser controlados por uma configuração de privacidade?

Para qualquer dado de geolocalização que você precise tratar, a fim de fornecer seu serviço principal, não é apropriado ter uma configuração de privacidade (pois sem o tratamento não há serviço principal a ser fornecido). Por exemplo, os serviços de mapas podem precisar saber a localização do usuário com o intuito de exibir corretamente o mapa necessário ou direcionar o usuário para seu destino escolhido.

No entanto, você deve oferecer às crianças controle sobre se e como seus dados pessoais são utilizados, sempre que possível. Portanto, qualquer serviço de geolocalização que vá além de seu serviço principal deve estar sujeito a uma configuração de privacidade. Por exemplo, serviços de mapeamento aprimorados que fazem recomendações para locais a serem visitados, com base na localização.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Assegurar que as opções de geolocalização estejam desativadas por padrão

Qualquer configuração de privacidade de geolocalização que você proporcionar deve ser desativada por padrão; com as crianças tendo que alterar ativamente a configuração padrão para permitir que seus dados de geolocalização sejam usados. A exceção a isso é se você puder demonstrar uma razão convincente para que uma opção de geolocalização seja ativada por padrão, levando em conta o melhor interesse da criança. Por exemplo, você pode argumentar que as métricas necessárias para medir a demanda de serviços regionais podem ser suficientemente não intrusivas para serem garantidas (levando em conta o melhor interesse da criança).

Você também deve considerar em que nível de granularidade o local precisa ser rastreado para fornecer cada recurso de seu serviço. Não colete mais detalhes granulares do que você realmente precisa e ofereça diferentes configurações, para diferentes níveis de serviço, se apropriado.

Deixar claro para a criança que sua localização está sendo rastreada

Você deve providenciar informações no momento da inscrição, e cada vez que o serviço for acessado, alertando a criança para o uso de dados de geolocalização e estimulando-a a discutir isso com um adulto de confiança, caso não entenda o que significa.

Você também deve fornecer uma indicação clara de quando a localização da criança está e quando não está sendo rastreada (por exemplo, pelo uso de um símbolo claro e visível para o usuário) e garantir que o rastreamento de localização não possa permanecer em modo ativado inadvertidamente ou por engano.

Reverter as configurações que tornam a localização da criança visível aos outros para 'desativada', após cada uso

Você deve assegurar que qualquer opção que torne a localização da criança visível aos outros esteja sujeita a uma configuração de privacidade que reverta para 'desativada', após cada sessão. A exceção a isso é se você puder demonstrar que tem uma razão convincente para fazer o contrário, levando em conta o melhor interesse da criança.

E o Regulamento de Privacidade e Comunicações Eletrônicas (RPCE)?

Se os dados de geolocalização que você está tratando também atenderem à definição de 'dados de localização' no RPCE, então você deve consultar nosso Guia sobre o RPCE para maiores orientações, pois há requisitos específicos do RPCE que você tem que cumprir.

Os dados de localização são definidos como:

> "qualquer dado tratado em uma rede de comunicações eletrônicas ou por um serviço de comunicações eletrônicas indicando a posição geográfica do equipamento terminal de um usuário de um serviço público de comunicações eletrônicas, incluindo dados relativos –
>
> (f) à latitude, à longitude ou à altitude do equipamento terminal;
>
> (g) à direção de viagem do usuário; ou
>
> (h) à hora em que as informações de localização foram registradas".

Ou seja, são informações coletadas por uma rede ou por um serviço acerca de onde o telefone ou outro dispositivo do usuário se encontra ou de onde foi localizado. Por exemplo, rastrear a localização de um telefone celular, a partir de dados coletados por estações de rádio em uma rede de telefonia móvel.

As regras do RPCE, geralmente, não incluem informações de localização baseadas em GPS de smartphones, tablets, navegação de satélite ou outros dispositivos, pois esses dados são criados e coletados independentemente da rede ou do provedor de serviços. Também não incluem informações de localização coletadas em nível puramente local (por exemplo, por equipamentos wi-fi instalados por empresas que oferecem wi-fi em suas instalações).

Para leituras além deste código:

Guia ao RPCE - localização de dados

11. CONTROLES PARENTAIS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Se você providenciar controles parentais, forneça à criança informações apropriadas à idade sobre isso. Se seu serviço on-line permitir que um pai ou um responsável monitore a atividade on-line de sua criança ou rastreie sua localização, disponibilize um sinal óbvio para a criança, quando ela estiver sendo monitorada.

O que se quer dizer com 'controles parentais'?

Os controles parentais são ferramentas que permitem aos pais ou responsáveis colocar limites à atividade on-line de uma criança e, dessa forma, mitigar os riscos aos quais a criança pode estar exposta. Eles incluem coisas como estabelecer limites de tempo ou horário de dormir, restringir o acesso à internet apenas a sites pré-aprovados e restringir as compras no sistema. Eles também podem ser usados para monitorar a atividade on-line de uma criança ou para rastrear sua localização física.

Por que os controles são importantes?

Eles são importantes porque podem ser usados para auxiliar os pais na proteção e na promoção do melhor interesse de seus filhos, um papel reconhecido pela CNUDC e discutido na seção deste código sobre o melhor interesse da criança.

No entanto, os controles parentais também têm impacto no direito à privacidade da criança, reconhecido pelo Artigo 16, da mesma convenção, e em seus direitos de associação, brincadeira, acesso à informação e liberdade de expressão. As crianças que estão sujeitas ao monitoramento persistente dos pais podem ter um senso diminuído de seu próprio espaço privado, o que pode afetar o desenvolvimento de seu senso em relação à própria identidade. Esse é, particularmente, o caso, à medida que a criança amadurece e sua expectativa de privacidade aumenta.

O Artigo 5(1)(a), do RGPD, exige que qualquer tratamento de dados pessoais seja lícito, leal e transparente.

> "5(1) Dados pessoais serão:
>
> Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência');"

Como podemos ter certeza de que conseguimos cumprir este padrão?

Deixar claro para a criança quando os controles parentais estiverem ativados e se elas estão sendo rastreadas ou monitoradas.

Se você providenciar controles parentais, então você deve providenciar informações apropriadas à idade, para que a criança saiba que os controles parentais estão em vigor.

Se seu serviço on-line permite o monitoramento ou o rastreamento de uma criança pelos pais, você deve fornecer recursos apropriados à idade para explicar o serviço à criança, a fim de que ela esteja ciente de que sua atividade está sendo monitorada por seus pais ou sua localização rastreada. Você deve apresentar um sinal claro e óbvio para a criança (como um ícone iluminado) que permita que ela saiba quando o monitoramento ou o rastreamento estiver ativo.

Você também deve providenciar aos pais informações sobre o direito à privacidade da criança tutelado pela CNUDC e os recursos para apoiar discussões entre pais e filhos que seja apropriada à idade da criança em questão.

A tabela a seguir fornece algumas diretrizes sobre o tipo de informação que você pode desejar disponibilizar e como você pode disponibilizá-la. São apenas um ponto de partida e você está livre para desenvolver suas próprias diretrizes, específicas para seu serviço e de acordo com cada usuário, desde que esteja de acordo com o padrão em destaque.

Você também deve considerar quaisquer responsabilidades adicionais que possa ter em relação à legislação de igualdade aplicável para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

FAIXA ETÁRIA	RECOMENDAÇÕES
0-5 Pré-alfabetização e alfabetização fundamental	Providenciar materiais de áudio ou vídeo para a criança, explicando que os pais estão sendo informados sobre o que fazem on-line, para fins de segurança e proteção. Providenciar materiais para os pais, explicando o direito da criança à privacidade, tutelado pela CNUDC, e como suas expectativas sobre isso, provavelmente, aumentarão à medida que forem crescendo. Providenciar um sinal claro e óbvio que indique quando o monitoramento ou o rastreamento está ativo.
6-9 Os principais anos do ensino fundamental	Providenciar materiais de áudio ou vídeo para a criança, explicando que os pais estão sendo informados sobre o que fazem on-line, para fins de segurança e proteção. Providenciar materiais para os pais explicando o direito da criança à privacidade, tutelado pela CNUDC, e como suas expectativas sobre isso, provavelmente, aumentarão à medida que forem crescendo. Providenciar recursos para ajudar os pais a explicar o serviço a seus filhos e discutir questões de privacidade com eles. Providenciar um sinal claro e óbvio que indique quando o monitoramento ou o rastreamento está ativo.

10-12 Anos de transição escolar	Providenciar materiais de áudio ou vídeo para a criança, explicando que os pais estão sendo informados sobre o que fazem on-line, para fins de segurança e proteção. Providenciar materiais para os pais explicando o direito da criança à privacidade, tutelado pela CNUDC, e como suas expectativas sobre isso, provavelmente, aumentarão à medida que forem crescendo. Providenciar recursos para ajudar os pais a explicar o serviço a seus filhos e discutir questões de privacidade com eles. Providenciar recursos que sejam adequados para uma criança usar de forma independente e que expliquem o serviço e os direitos de privacidade envolvidos. Providenciar um sinal claro e óbvio que indique quando o monitoramento ou o rastreamento está ativo.
13-15 Início da adolescência	Providenciar material de áudio, vídeo ou por escrito para a criança, explicando como funciona seu serviço e o equilíbrio entre os direitos de privacidade dos pais e da criança. Providenciar materiais para os pais, explicando o direito da criança à privacidade, tutelado pela CNUDC. Providenciar um sinal claro e óbvio que indique quando o monitoramento ou o rastreamento está ativo.
16-17 Aproximando-se da maioridade	Providenciar materiais de áudio ou vídeo para a criança, explicando que os pais estão sendo informados sobre o que fazem on-line, para fins de segurança e proteção. Providenciar materiais para os pais explicando o direito da criança à privacidade, tutelado pela CNUDC, e como suas expectativas sobre isso, provavelmente, aumentarão à medida que forem crescendo. Providenciar recursos para ajudar os pais a explicar o serviço a seus filhos e discutir questões de privacidade com eles. Providenciar recursos que sejam adequados para uma criança usar de forma independente e que expliquem o serviço e os direitos de privacidade envolvidos. Providenciar um sinal claro e óbvio que indique quando o monitoramento ou o rastreamento está ativo.

12. PERFILAMENTO (*PROFILING*)

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Ativar opções que utilizam o perfilamento 'desativado' por padrão (a menos que você possa demonstrar uma razão convincente para que o perfilamento esteja ativado por padrão, levando em conta o melhor interesse da criança). Só permitir o perfilamento se você tiver medidas adequadas para proteger a criança de quaisquer efeitos nocivos (em particular, sendo proporcionado conteúdo prejudicial à sua saúde ou ao seu bem-estar).

O que se quer dizer com 'perfilamento'?

Perfilamento é definido no RGPD:

"qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos de uma pessoa natural, nomeadamente para analisar ou prever aspectos relacionados ao seu desempenho profissional, à sua situação econômica, à sua saúde, às suas preferências pessoais, aos seus interesses, à sua confiabilidade, ao seu comportamento, à sua localização ou aos seus deslocamentos".

O perfilamento pode ser usado para uma ampla variedade de finalidades. Pode ser usado, extensivamente, em um contexto on-line, para sugerir ou oferecer conteúdo aos usuários, para determinar onde, quando e com que frequência esse conteúdo deve ser oferecido, para incentivar os usuários a adotar comportamentos ou para identificar usuários como pertencentes a grupos particulares. Também pode ser usado para ajudar a estabelecer ou estimar a idade de um usuário (conforme detalhado no padrão sobre aplicação adequada à idade) ou para proteção de crianças, combate ao terrorismo, ou prevenção de crimes.

Os perfilamentos são, geralmente, baseados no histórico de atividades on-line ou no histórico de navegação de um usuário. Eles podem ser criados usando dados pessoais coletados diretamente ou através de inferências (por exemplo, preferências ou características inferidas a partir de associações com outros usuários ou de escolhas on-line passadas).

Os feeds de conteúdo baseados em perfilamentos podem incluir conteúdo publicitário, conteúdo fornecido por outros sites, downloads, conteúdo gerado por outros usuários da internet, conteúdo escrito, auditivo ou visual. Ele também pode ser usado para sugerir outros usuários para "conectar-se" ou "seguir".

Por que isso é importante?

O perfilamento de dados é mencionado no Considerando 38, do RGPD, como uma área na qual as crianças merecem proteção específica, no que diz respeito ao uso de seus dados pessoais.

Há também regras específicas no artigo 22, do RGPD, sobre decisões (incluindo perfilamento) que se baseiam, exclusivamente, no tratamento automatizado de dados pessoais e que têm um efeito legal ou similar significativo sobre o titular de dados.

> "22(1) O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada, exclusivamente, com base no tratamento automatizado, incluindo o perfilamento, que resulte em consequências legais a seu respeito ou que o afete de forma semelhante".

O Considerando 71, do RGPD, determina que essas decisões 'não devem dizer respeito a uma criança'.

O princípio da licitude, lealdade e transparência, do Artigo 5(1), também é relevante, porque esta é uma área na qual ocorre o chamado 'tratamento invisível'. Assim, é mais difícil ainda para as crianças compreenderem como seus dados pessoais estão sendo utilizados e quais as consequências dessa utilização.

> "22(1) O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada, exclusivamente, com base no tratamento automatizado, incluindo o perfilamento, que resulte em consequências legais a seu respeito ou que o afete de forma semelhante".

Alguns tipos de perfilamento podem ser relativamente positivos, por exemplo, a personalização de um ambiente on-line de um software ou de uma plataforma, para incorporar um tema animal no conteúdo exibido. Outros perfilamentos, como, por exemplo, conteúdos que, gradualmente, levam a criança para longe de sua área de interesse original, para conteúdos menos adequados, suscitam preocupações muito mais significativas.

Todos os tipos de perfilamento devem ser controlados por configurações de privacidade?

É importante lembrar que 'desativado por padrão' não significa que não seja possível o perfilamento ou que ele seja banido. Seguindo as proteções e os passos estabelecidos nesta seção, que podem incluir, por exemplo, o consentimento efetivo, é possível habilitar o perfilamento, utilizando os dados pessoais de crianças, de forma segura e leal.

Não faz sentido oferecer uma configuração de privacidade, se o perfilamento for essencial para a prestação do serviço principal que a criança solicitou. Isso porque, se o perfilamento fosse desativado, não haveria nenhum serviço residual para a criança utilizar. Esse conceito deve ser interpretado de forma restrita, ou seja, no sentido de que ele é completamente intrínseco ao serviço.

Entretanto, sempre que possível, você deve oferecer às crianças o controle sobre se e como seus dados pessoais são utilizados. Portanto, a maioria dos perfilamentos devem estar sujeitos a uma configuração de privacidade. Se você puder fornecer um serviço central ou residual sem o perfilamento, então você deve fornecer uma configuração de privacidade para quaisquer aspectos adicionais de seu serviço que dependam do perfilamento.

Você deve sempre fornecer uma configuração de privacidade para publicidade comportamental que é usada para financiar um serviço, mas não faz parte do serviço principal que a criança deseja acessar. Embora possam haver alguns exemplos limitados de serviços em que a publicidade comportamental faz parte do serviço principal (por exemplo, um voucher ou um serviço com desconto / promoção), entendemos que serão excepcionais. Na maioria dos casos, o modelo de financiamento será distinto do serviço principal e, portanto, deve estar sujeito a uma configuração de privacidade que é 'desativada' por padrão.

Também podem haver algumas outras circunstâncias limitadas em que não será apropriado oferecer uma configuração de privacidade sobre o perfilamento. Por exemplo, se você estiver fazendo um perfilamento, a fim de cumprir uma exigência legal ou regulatória (como uma exigência de proteção ou proteção de crianças), para prevenir a exploração ou o abuso sexual infantil on-line ou para assegurar a idade, com a finalidade de que você possa aplicar corretamente as disposições deste código a usuários infantis.

Como isso se encaixa nos requisitos do RPCE?

O perfilamento pode depender do uso de *cookies* e de tecnologias similares para armazenar ou salvar as informações sobre a atividade on-line anterior de um usuário.

Um cookie é um pequeno arquivo de texto que é baixado em 'equipamento terminal' (por exemplo, um computador ou um smartphone), quando o usuário acessa um site. Ele permite que o site reconheça o dispositivo do usuário e armazene algumas informações sobre as preferências do usuário ou as atividades passadas.

O RPCE exige que forneça aos usuários informações claras e compreensíveis sobre o uso de *cookies* e obtenha o consentimento prévio para qualquer uso que seja 'não essencial'.

Portanto, se você usa *cookies* para fins de perfilamento, você precisa considerar as regras do RPCE para a definição do cookie, bem como o RGPD e este código para o tratamento subjacente de dados pessoais (perfilamento) que o cookie suporta ou habilita.

Perfilamento e *cookies* não essenciais

Se o cookie não for essencial para providenciar o serviço que a criança quer acessar, então o perfilamento subjacente que ele facilita normalmente precisa estar sujeito a uma configuração de privacidade. Isso dá à criança o controle sobre se seus dados pessoais são utilizados para aquele fim.

É necessário o consentimento para o cookie, bem como uma base legal do RGPD para qualquer tipo de tratamento, para fins de um tratamento subjacente (na prática, isso também pode ser consentimento).

Cookies, perfilamento, e serviços principais

Se o cookie é essencial para o fornecimento de seu serviço principal, então é provável que o perfilamento subjacente que o cookie permite também o seja. Nessa circunstância, providenciar uma configuração de privacidade que permita à criança controlar se seus dados pessoais são utilizados para aquele fim não será adequado. Você precisa de uma base legal (além do consentimento) para o tratamento subjacente (perfilamento) e não precisará do consentimento para o cookie.

Cookies, perfilamento e serviços não essenciais

Os *cookies* também podem ser fundamentais para a prestação de seus serviços não essenciais. No entanto, como aqueles são elementos opcionais de seu serviço, você precisa, primeiramente, fornecer uma configuração de privacidade que dê à criança o controle sobre se ela deseja que seus dados pessoais sejam processados, para só depois ter acesso a eles.

Se a criança decidir assim proceder, então você não precisa do consentimento para o uso do cookie – já que a criança está solicitando, especificamente, o acesso a parte de seu serviço e o cookie é estritamente necessário para esse fim.

No entanto, você precisa de uma base legal para o tratamento subjacente.

Cookies, perfilamento e estimativa de idade ou garantia de idade

Você também pode utilizar *cookies* para o perfilamento que pretende cumprir as exigências implícitas de verificação de idade do Artigo 8, do RGPD, ou para garantir a idade, a fim de aplicar adequadamente os parâmetros deste código. Para mais detalhes sobre os requisitos do Artigo 8, veja o Anexo C - Bases legais para o tratamento.

Nessa circunstância, a finalidade para a qual você utiliza os *cookies* é considerada essencial para o serviço, pois você precisa utilizá-lo para fornecer um serviço adequado à idade e cumprir com o RGPD. A criança não precisará consentir com o cookie, desde que o cookie em questão seja utilizado exclusivamente para essa finalidade, e não para qualquer outra.

Para maiores informações sobre *cookies*, e quando um cookie é essencial e não essencial, veja nossas orientações sobre *Cookies* e tecnologias similares.

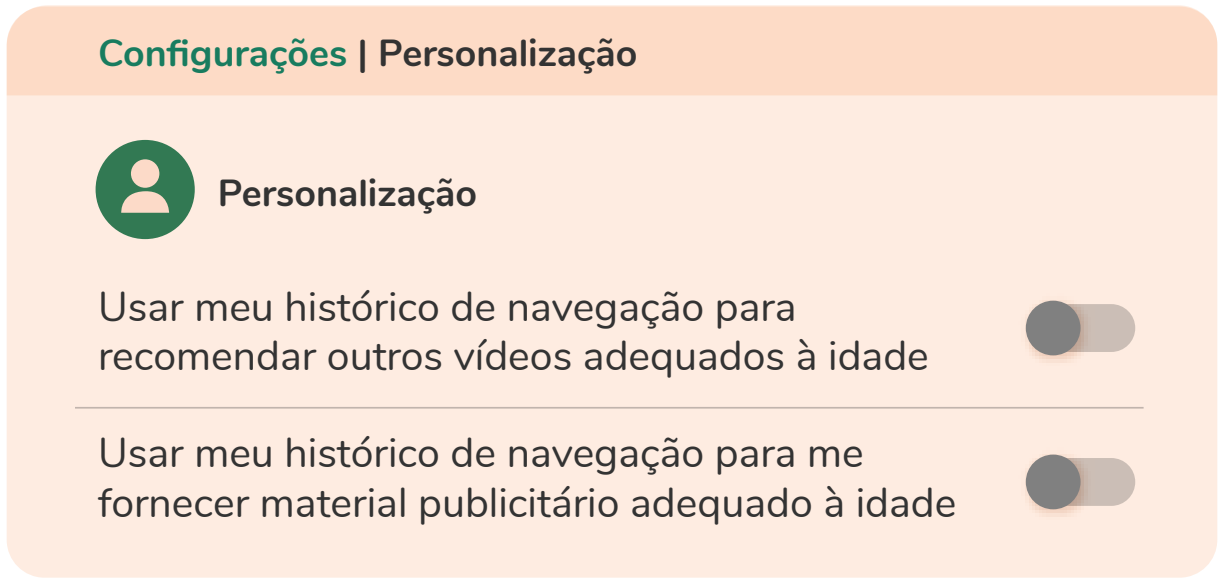
Como podemos ter certeza de que conseguimos cumprir este padrão?

Distinguir os diferentes tipos de perfilamentos para propósitos distintos

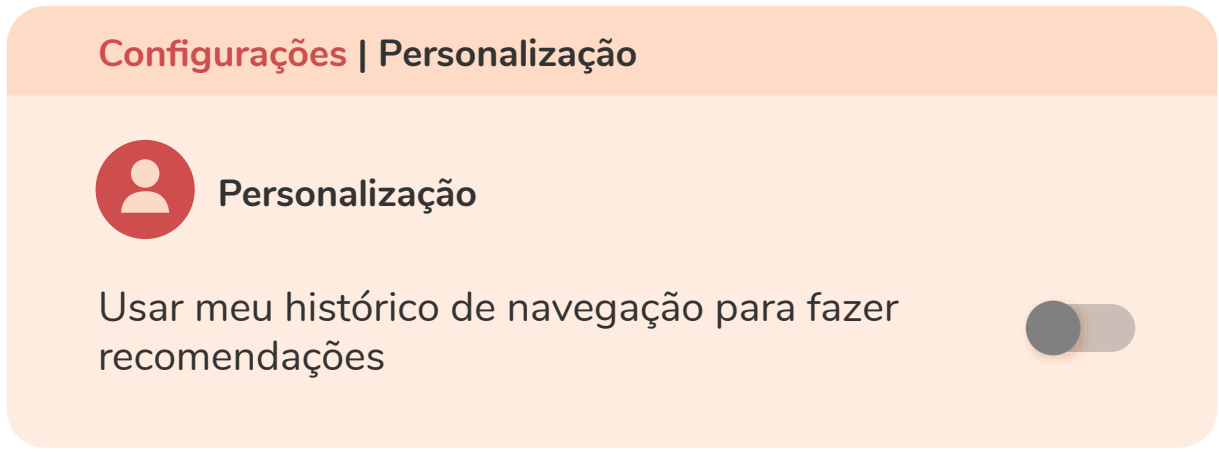
Como o perfilamento pode ser usado para servir a uma ampla gama de propósitos, é extremamente importante ser claro sobre as finalidades para as quais seu serviço usa dados pessoais com a intenção de traçar o perfil dos usuários e diferenciá-los. Propósitos, como os de oferecer um ‘serviço personalizado’, não são suficientemente específicos.

Onde for apropriado oferecer configurações de privacidade, você deve oferecer configurações separadas para cada tipo diferente de perfilamento. Não é aceitável agrupar diferentes tipos de perfilamento sob uma configuração de privacidade ou agrupar diferentes tipos de perfilamento com tratamento para outros fins.

Práticas aceitáveis:



Práticas inaceitáveis:



Assegurar que os recursos que dependem do perfilamento sejam desativados por padrão (a menos que haja uma razão convincente para fazer o contrário)

Você precisa substituir quaisquer opções dentro de seu serviço que dependam do perfilamento por padrão, a menos que você possa demonstrar uma razão convincente para que esse não seja o caso, levando em conta o melhor interesse da criança. Você precisa avaliar isso nas circunstâncias específicas de seu tratamento.

Na prática, isso provavelmente significa que quaisquer características não essenciais que dependam do perfilamento, e que você forneça para fins comerciais, estão sujeitas a uma configuração de privacidade que é desativada por padrão.

No caso de qualquer perfilamento que você faça para fins de publicidade comportamental, que é facilitado por *cookies*, essa abordagem é mencionada nos comentários do Comité Europeu para a Proteção de

Dados (CEPD)[17]. O CEPD indicou que 'interesses legítimos' dificilmente fornecem uma base legal válida para o tratamento para aquele fim, o que significa que o consentimento é sua única base viável para o tratamento. Como o consentimento válido tem que ser '*opt-in*', permitir um perfilamento 'por padrão' não é uma opção. Você também precisa cumprir os requisitos do Artigo 8, do RGPD, que dispõe sobre a necessidade de consentimento dos pais, se a criança tiver menos de 13 anos de idade. Para mais informações sobre bases legais para o tratamento e os requisitos do Artigo 8, consulte o Anexo C.

No entanto, você pode ter um argumento contundente de que você precisa ativar as opções de perfilamento por padrão para outros propósitos.

Por exemplo, o perfilamento pode ser apropriado para assegurar que um serviço acessível a uma criança deficiente (por exemplo, identificar que uma criança tem uma necessidade contínua de um serviço legendado, assinado ou outro serviço apoiado) seja ativado por padrão.

Existe a possibilidade de que você consiga demonstrar que o perfilamento para fins de informar conteúdo deva ser permitido por padrão, para reconhecer os direitos das crianças de acesso à informação. Embora você ainda precise do consentimento para definir os *cookies* que apoiam o perfilamento de acordo com as exigências do RPCE. Esse é o caso mais provável, se você puder demonstrar que está em conformidade com os códigos de prática regulatórios existentes que regem o conteúdo e as práticas da mídia (como o Código de Prática dos Editores) e tem controle editorial sobre o conteúdo a que as crianças terão acesso, como resultado do perfilamento. É pouco provável que isso se aplique, no caso de você não ter o controle editorial ou não aderir a outros controles regulatórios. Veja também nossas FAQs destinadas aos veículos de comunicação.

Proporcionar intervenções apropriadas, quando qualquer tipo de perfilamento for ativado

No momento em que qualquer opção de perfilamento for ativada, você precisa fornecer informações adequadas à idade sobre o que acontecerá com os dados pessoais da criança e quaisquer riscos inerentes a esse tratamento.

Você também deve fornecer avisos adequados à idade para buscar a assistência de um adulto e não ativar o perfilamento, se a criança, em questão, não tiver certeza do que se trata ou não entender.

17. Em inglês: *European Data Protection Board* - EDPB.

Dependendo de sua avaliação de risco e da idade da criança, pode ser interessante fazer outras intervenções, que podem incluir outras medidas de controle e garantia de idade.

Se o perfilamento estiver ativado, assegure-se de que você implemente medidas adequadas para proteger a criança (em particular, de conteúdo inadequado)

Se seu serviço on-line utiliza algum tipo de perfilamento, então você precisa tomar as medidas apropriadas para garantir que isso não resulte em danos para a criança.

Na prática, isso significa que, se você utilizar o perfilamento em crianças (usando seus dados pessoais) para sugerir-lhes conteúdo, então você precisa de medidas adequadas para assegurar que conteúdos prejudiciais à saúde física ou mental ou ao bem-estar das crianças não cheguem até elas, sempre considerando a idade da criança em questão. Como abordado na seção deste código sobre RIPDs, testar seus algoritmos deve ajudá-lo a avaliar a eficácia de suas medidas.

Essas medidas podem incluir *tagging* contextual, procedimentos robustos de notificação e elementos de moderação humana. Poderia também incluir seus próprios controles editoriais sobre o conteúdo exibido, incluindo a adesão a códigos de conduta ou outras disposições regulatórias (como o cumprimento do Código de Práticas dos Editores ou do Código de Veiculação da Ofcom)[18]. Reconhecemos a importância dos direitos das crianças de acessar informações da mídia, e os benefícios sociais e de desenvolvimento, ao poderem se engajar em assuntos atuais e no mundo ao seu redor. Portanto, aceitamos que a adesão aos códigos de conduta editoriais ou de radiodifusão nega a necessidade de os provedores de notícias on-line tomarem quaisquer medidas adicionais em relação ao conteúdo de notícias para crianças. Veja também nossas FAQs destinadas aos veículos de comunicação.

Se você estiver usando os dados pessoais das crianças para recomendar automaticamente o conteúdo a elas com base em seu histórico de uso/navegação, então você é responsável pelas recomendações que fizer. Isso se aplica, mesmo que o conteúdo em si seja gerado pelo usuário. Em termos de proteção de dados, você tem uma responsabilidade maior nessa situação do que se a criança pesquisasse proativamente esse conteúdo por conta própria. Isso porque é seu tratamento de dados pessoais que entrega o conteúdo à criança. A lei de proteção de dados não o torna responsável pelo conteúdo de terceiros, mas o torna

18. *The Editors' Code of Practice, or the Ofcom Broadcasting Code*. Disponível em: <https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code>. Acesso em 27 de maio de 2021.

responsável pelo conteúdo que você fornece às crianças que utilizam seu serviço, com base no uso de seus dados pessoais.

Sua abordagem, de modo geral, deve ser que, se o conteúdo o qual você promove ou os comportamentos os quais seus recursos encorajam são obviamente prejudiciais, ou são reconhecidos como prejudiciais para a criança, em um contexto (por exemplo, de regras de marketing, classificação de filmes, conselhos de fontes oficiais do governo, como conselhos de Oficiais Médicos Chefes do Reino Unido, classificações da Informação Pan-Europeia de Jogos (PEGI)[19], então você deve assumir que o mesmo tipo de conteúdo ou comportamento é prejudicial em outros contextos. Quando a evidência for inconclusiva, você deve aplicar o mesmo princípio de precaução.

Conteúdos ou comportamentos que podem ser prejudiciais à saúde e ao bem-estar das crianças (levando em conta sua idade) incluem:

- publicidade ou conteúdo de marketing que seja contrário às diretrizes do Comitê de Prática Publicitárias para Crianças (CPP)[20];
- filme ou conteúdo televisivo sob demanda que é classificado como inadequado para a faixa etária em questão;
- conteúdo musical que é rotulado com 'aconselhamento parental' (*parental advisory*) ou 'material explícito';
- pornografia ou outro conteúdo adulto ou violento;
- conteúdo gerado pelo usuário (conteúdo que é postado por outros usuários da internet) que é obviamente prejudicial ao bem-estar das crianças ou é formalmente reconhecido dessa forma (por exemplo, conteúdo pró-suicídio, pró-autoagressão, pró-anorexia. Conteúdo que represente ou defenda um comportamento arriscado ou perigoso para crianças); e
- estratégias utilizadas para ampliar o envolvimento do usuário, como, por exemplo, notificações cronometradas que respondem à inatividade.

Portanto, se você acredita que não é viável para você colocar medidas adequadas em prática, então você não poderá traçar o perfil das crianças, para fins de recomendação de conteúdo on-line. Nessa circunstância, você precisa ter certeza de que as crianças não podem alterar nenhuma configuração de privacidade que permita esse tipo de perfilamento.

---

19. PEGI é a sigla oficial é inglês: Pan European Game Information.

20. *Committee of Advertising Practice (CAP)*. Disponível em: <https://www.asa.org.uk/about-asa-and-cap.htm>. Acesso em 27 de maio de 2021.

Da mesma forma, se não for possível estabelecer medidas adequadas para proteger as crianças dos danos decorrentes do perfilamento para outros propósitos (como o perfilamento para promover certos comportamentos), também não se deve fazer o perfilamento de crianças para esses fins.

Como isso se encaixa com outras regras sobre restrição de acesso ao conteúdo para crianças?

Talvez seja necessário observar outras regras para restringir o acesso ao conteúdo, a fim de assegurar que você não utilize os dados pessoais das crianças de uma forma que seja prejudicial ao seu bem-estar (para mais detalhes, consulte o padrão sobre o uso indevido de dados).

O Comitê de Práticas Publicitárias (CAP, na sigla em inglês) exige que, quando a publicidade for dirigida através do uso de dados pessoais, os anunciantes devem mostrar que tomaram medidas razoáveis para reduzir a probabilidade de que aqueles os quais estão, ou têm probabilidade de estar, em uma categoria etária protegida sejam expostos a conteúdo de marketing restrito à idade.

A autoridade reguladora de comunicações, Ofcom, em suas regras sobre Serviços 'sob demanda', requer que os provedores de conteúdo 'sob demanda' disponibilizem apenas conteúdos determinados ('material restrito'), se puderem fazê-lo de uma forma que assegure que aqueles com menos de 18 anos de idade não poderão acessá-lo de forma livre e irrestrita.

A Diretiva de Serviços de Mídia Audiovisual de 2018 (AVMSD, na sigla em inglês)[21] (se implementada no Reino Unido) exigirá que 'serviços de plataforma de compartilhamento de vídeo' utilizem medidas proporcionais, em relação ao modo como eles organizam o conteúdo que compartilham, para proteger menores de conteúdo que possa prejudicar seu desenvolvimento físico, mental ou moral.

Consideramos que é condizente com essas disposições permitir que os dados pessoais das crianças só sejam utilizados para determinar o conteúdo que será entregue se você puder colocar em prática medidas adequadas para evitar que elas tenham acesso a conteúdos prejudiciais à sua saúde e ao seu bem-estar.

A AVMSD também exige que você não utilize os dados pessoais coletados ou gerados com o objetivo de proteger menores de idade de conteúdos que possam prejudicar seu desenvolvimento físico, mental ou moral para fins comerciais, como marketing direto, perfilamento e publicidade direcionada por comportamento.

---

21. Em inglês: Audiovisual Media Services Directive (AVMSD). Disponível em: <https://ec.europa.eu/digital-single-market/en/audiovisual-media-services-directive-avmsd>. Acesso em 20 de abril de 2020.

Consideramos que essa exigência é consistente com o princípio da limitação da finalidade do RGPD e com nossa orientação, nas seções deste código, sobre aplicação adequada à idade – E se precisarmos coletar dados pessoais, a fim de estabelecer a idade? Isso não significa que os serviços dentro do escopo da AVMSD não possam jamais tratar dados pessoais para fins comerciais. Significa apenas que você não pode usar os dados pessoais coletados para uma finalidade, para outra. Se esses serviços desejarem fazer o perfilamento de crianças com o fim de publicidade comportamental, você precisará do consentimento da criança (ou dos pais). Para mais informações sobre consentimento, consulte o Anexo C Bases legais para tratamento.

Trabalharemos com outros órgãos regulatórios conforme necessário, quando surgirem questões de consistência regulatória.

Para leituras além deste código:

Código de Práticas dos Editores

O Código de Radiodifusão Ofcom (com o Código de Promoção Cruzada e as Regras de Serviço de Programas Sob Demanda)

Diretiva (UE) 2018/1808 que altera a Diretiva 2010/13/EU (Diretiva de Serviços de Mídia Audiovisual) e o documento de consulta do governo britânico sobre Veículos de Comunicação Audiovisual

FAQs sobre o código de *design* adequado à idade destinadas aos veículos de comunicação.

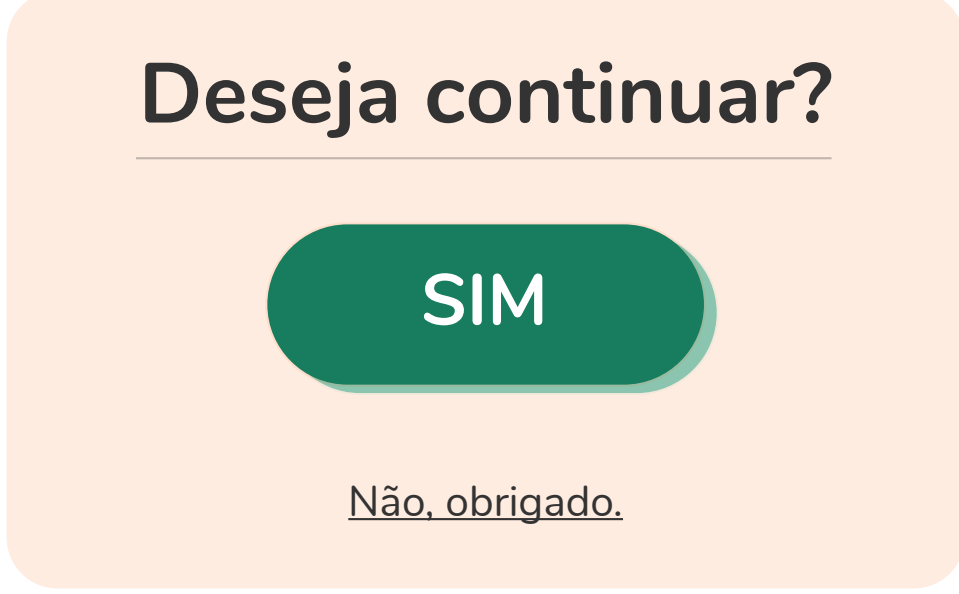
13. TÉCNICAS DE *NUDGE*

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

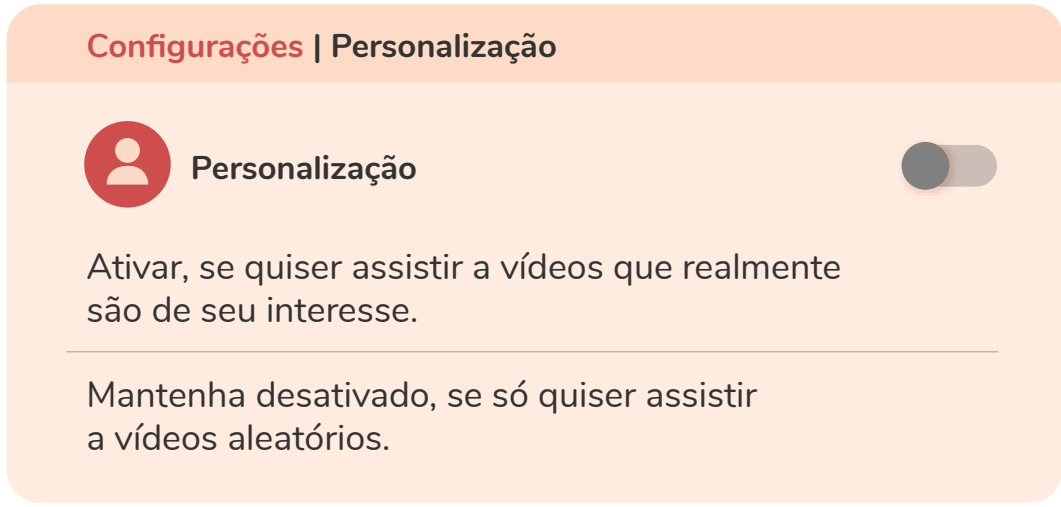
Não usar técnicas de Nudge para conduzir ou encorajar crianças a fornecer dados pessoais desnecessários ou a enfraquecer ou desativar suas proteções de privacidade.

O que se quer dizer com 'técnicas de nudge'?

Técnicas de nudge são características de *design* que levam ou incentivam os usuários a seguir os caminhos de preferência do *designer* no processo de decisão do usuário. Por exemplo, no gráfico abaixo, o grande botão verde 'sim' é apresentado de forma muito mais proeminente do que a opção de impressão pequena 'não'. Assim, o usuário é "*nudged*" ou encorajado a responder 'sim' em vez de 'não', independentemente da opção que esteja sendo apresentada.



No exemplo seguinte, a linguagem usada a fim de explicar as consequências de duas alternativas é estruturada mais positivamente para uma alternativa do que para a outra, mais uma vez encorajando ou 'empurrando' o usuário a optar pela opção de preferência do provedor de serviços.



Uma outra técnica de *nudge* envolve fazer uma opção muito menos incômoda ou demorada do que a alternativa, encorajando, portanto, muitos usuários a optarem pela opção mais fácil. Por exemplo, oferecer uma opção de privacidade baixa instantaneamente, com apenas um 'clique', e a alternativa de privacidade alta, através de um mecanismo de seis cliques, ou com um atraso no acesso ao serviço.

Por que isso é importante?

O Artigo 5(1)(a), do RGPD, exige que os dados pessoais sejam:

> "tratados de forma lícita, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência')"

E o Considerando 38, do RGPD, determina que:

> "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das garantias em questão e dos seus direitos relacionados com o tratamentos dos dados pessoais..."

O uso de técnicas de *nudge* no *design* de serviços on-line pode ser usado para induzir os usuários, incluindo crianças, a fornecerem mais dados pessoais para acesso a serviços on-line do que eles normalmente ofereceriam de forma voluntária. Da mesma forma, essa técnica pode ser usada para conduzir os usuários, particularmente as crianças, a selecionar escolhas menos privativas, ao personalizarem suas configurações de privacidade.

O uso de técnicas baseadas na exploração de vieses psicológicos humanos dessa forma vai contra as disposições de 'lealdade' e 'transparência', do RGPD, bem como as considerações específicas da criança, expostas no Considerando 38.

Como podemos ter certeza de que conseguimos cumprir este padrão?

Não usar técnicas de *nudge* para induzir as crianças a tomar decisões de privacidade inadequadas

Você não deve usar técnicas de *nudge* para induzir as crianças a ativar opções que signifiquem uma maior exposição de dados pessoais ou ainda que as levem a desativar proteções de privacidade.

Não se deve explorar processos psicológicos inconscientes para esse fim (como associações entre certas cores ou imagens e consequências positivas, ou necessidades de afirmação humana).

Não se deve usar técnicas de *nudge* que possam induzir as crianças a mentir sobre sua idade. Por exemplo, pré-selecionar uma faixa etária mais velha para elas ou não lhes permitir a opção de selecionar sua verdadeira faixa etária.

Usar *nudges* que são pró-privacidade quando for adequado

Ao pensar no melhor interesse da criança como uma consideração primordial, seu *design* deve atender às necessidades de desenvolvimento da idade dos seus usuários crianças.

Crianças mais novas, com níveis limitados de compreensão e capacidade de decisão, precisam de mais intervenções baseadas em instrução, de menos explicações, de regras claras a seguir e de um maior nível de apoio dos pais. O *nudge* ou o 'empurrão' que leva a opções de alta privacidade, a comportamentos que melhoram o bem-estar e ao controle e ao envolvimento dos pais deve contribuir para essas necessidades.

À medida que as crianças crescem, seu foco deve gradualmente se tornar apoiá-las no desenvolvimento de habilidades conscientes de tomada de decisão, fornecendo explicações claras sobre funcionalidade, riscos e consequências. Elas se beneficiarão de intervenções mais neutras, que exijam maior reflexão sobre as coisas. O apoio dos pais ainda pode ser necessário, mas você deve apresentá-lo como uma opção ao lado da sinalização para outros recursos.

Considerar o uso de técnicas de *nudges* para promover a saúde e o bem-estar

Você também deve considerar a possibilidade de usar técnicas de *nudges* em relação às crianças de forma a promover sua saúde e seu bem-estar. Por exemplo, incentivando-as a buscar recursos de apoio ou proporcionando mecanismos de 'pausar' e 'salvar'.

Se você usa dados pessoais para respaldar esses recursos, ainda precisa certificar-se de que seu tratamento está em conformidade com a lei (incluindo ter uma base legal para o tratamento e ter fornecido informações claras sobre privacidade), contudo, tendo se atentado a essas questões, é provável que o tratamento ocorrerá de forma leal, conforme previsto pelo RGPD.

A tabela abaixo apresenta algumas recomendações que você talvez deseje aplicar a crianças de diferentes idades. Embora, conforme já ressaltado, você esteja livre para desenvolver suas próprias recomendações, de acordo com o seu serviço específico, a jornada do usuário deve sempre seguir o parâmetro destacado no título.

Você também deve considerar quaisquer responsabilidades adicionais que possa ter, de acordo com obrigações assumidas perante a legislação de igualdade relevante para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

FAIXA ETÁRIA	RECOMENDAÇÕES
0-5 Pré-alfabetização e alfabetização fundamental	Proporcionar um design cuja arquitetura seja de alta privacidade por padrão. Se houver tentativa de mudança desse padrão, utilize um nudge para a manutenção de alta privacidade ou o envolvimento dos pais ou de um adulto de confiança. Evitar explicações – apresente em formato de regras, com o objetivo de proteger e de ajudar. Considerar outras intervenções, como notificações parentais, atrasos de ativação ou desativação de instalações para mudar as configurações de privacidade padrão, sem o envolvimento dos pais, dependendo dos riscos inerentes ao tratamento. Incluir nudges voltados ao bem-estar, para melhorar determinados comportamentos (como, por exemplo, fazer pausas, intervalos e descansar). Oferecer ferramentas que encorajem a melhoria do bem-estar (como pausa de nível médio e recursos que proporcionem ao usuário a opção de salvar a atividade em curso, como, por exemplo, dar pausa em um jogo on-line).
6-9 Os principais anos do ensino fundamental	Proporcionar um design, cuja arquitetura seja de alta privacidade por padrão. Se houver tentativa de mudança desse padrão, utilize um nudge para a manutenção de alta privacidade ou o envolvimento dos pais ou de um adulto de confiança. Fornecer explicações simples de funcionalidade e risco inerente, mas em formato de regras, com o intuito de proteger e ajudar. Considerar outras intervenções, como notificações parentais, atrasos de ativação ou desativação de instalações para mudar as configurações de privacidade padrão, sem o envolvimento dos pais, dependendo dos riscos inerentes ao tratamento. Incluir nudges voltados ao bem-estar, para melhorar determinados comportamentos (como, por exemplo, fazer pausas, intervalos e descansar). Oferecer ferramentas que encorajem a melhoria do bem-estar (como pausa de nível médio e recursos que proporcionem ao usuário a opção de salvar a atividade em curso, como, por exemplo, dar pausa em um jogo on-line).

10-12 Anos de transição escolar	Proporcionar um design cuja arquitetura seja de alta privacidade por padrão. Se houver tentativa de mudança desse padrão, providencie explicações sobre a funcionalidade e o risco inerente, e recomende o envolvimento dos pais ou de um adulto de confiança. Apresentar opções, de forma a incentivar a tomada de decisões conscientes. Considerar outras intervenções, como notificações parentais, atrasos de ativação ou desativação de instalações para mudar as configurações de privacidade padrão sem o envolvimento dos pais, dependendo dos riscos. Incluir nudges voltados ao bem-estar (como, por exemplo, fazer pausas ou intervalos). Oferecer ferramentas que encorajem a melhoria do bem-estar (como pausa de nível médio e recursos que proporcionem ao usuário a opção de salvar a atividade em curso, como, por exemplo, dar pausa em um jogo on-line).
13-15 Início da adolescência	Proporcionar um design cuja arquitetura seja de alta privacidade por padrão. Se houver tentativa de mudança desse padrão, providencie explicações sobre a funcionalidade e o risco inerente, e recomende o envolvimento dos pais ou de um adulto de confiança. Apresentar opções, de forma a incentivar a tomada de decisões conscientes. Considerar outras intervenções, como notificações parentais, atrasos de ativação ou desativação de instalações para mudar as configurações de privacidade padrão sem o envolvimento dos pais, dependendo dos riscos. Incluir nudges voltados ao bem-estar (como, por exemplo, fazer pausas ou intervalos). Oferecer ferramentas que encorajem a melhoria do bem-estar (como pausa de nível médio e recursos que proporcionem ao usuário a opção de salvar a atividade em curso, como, por exemplo, dar pausa em um jogo on-line).
16-17 Aproximando-se da maioridade	Proporcionar um design cuja arquitetura seja de alta privacidade por padrão. Fornecer explicações sobre a funcionalidade e o risco inerente. Apresentar opções de forma a incentivar a tomada de decisões conscientes. Incluir orientações para fontes de apoio, como os pais. Sugerir comportamentos que levam ao bem-estar (como, por exemplo, fazer pausas ou intervalos). Oferecer ferramentas que encorajem a melhoria do bem-estar (como pausa de nível médio e recursos que proporcionem ao usuário a opção de salvar a atividade em curso, como, por exemplo, dar pausa em um jogo on-line).

14. BRINQUEDOS E DISPOSITIVOS CONECTADOS

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Se você disponibilizar um brinquedo ou um dispositivo conectado, certifique-se de incluir ferramentas eficazes para permitir a conformidade com este código.

O que se quer dizer com 'brinquedos conectados e dispositivos'?

São brinquedos infantis e outros dispositivos que estão conectados à internet. São produtos físicos que são assistidos por alguma funcionalidade fornecida através de uma conexão com a internet. Por exemplo:

- um ursinho de pelúcia falante com um microfone que registra o que a criança está dizendo e depois envia esses dados de volta para seus servidores, a fim de que você possa usá-los para personalizar as respostas do ursinho de pelúcia;
- um monitor de atividade física (*fitness band*) que registra o nível de atividade física da criança e depois o transmite de volta para seus servidores, a fim de que a criança possa então acessar relatórios de atividades, através de um aplicativo de *fitness*; ou
- um dispositivo alto-falante interativo, chamado de '*home hub*', que fornece serviços baseados na internet através de um serviço de reconhecimento de voz.

Você precisa estar em conformidade com os parâmetros deste código, se você fornecer um brinquedo ou dispositivo que coleta e transmite os dados pessoais, através de uma conexão de rede dessa forma. Se você fornecer brinquedos ou dispositivos eletrônicos que não se conectam à internet, e apenas armazenam dados pessoais dentro do próprio dispositivo, este código não se aplica a você, pois você não tem acesso a nenhum dado pessoal.

Por que isso é importante?

Brinquedos e dispositivos conectados suscitam uma série de problemas, porque o escopo de coleta e o tratamento de dados pessoais deles, através de funções como câmeras e microfones, é considerável. Eles são frequentemente utilizados por várias pessoas de diferentes idades e por crianças muito pequenas, sem a supervisão de um adulto. Ofere-

cer transparência através de um produto físico, em vez de um produto baseado em tela, também pode ser um desafio particular.

No entanto, você ainda tem a responsabilidade de atender às exigências do RGPD e de garantir que seu tratamento seja legal, leal e transparente, conforme exigido pelo Artigo 5(1); portanto, você precisa ter certeza de que possui ferramentas que lhe permitam estar em conformidade com este código.

Como podemos ter certeza de que cumprimos este padrão?

Seja claro sobre quem está processando os dados pessoais e quais são suas responsabilidades

Se você disponibilizar um brinquedo ou um dispositivo conectado, então você precisa ser claro sobre quem irá tratar os dados pessoais que aquele transmite através da conexão de rede e quais são suas responsabilidades de proteção de dados.

Se você fornecer tanto o produto físico, quanto a funcionalidade on-line que o suporta, então você é o único responsável por garantir o tratamento em conformidade com este código. Se você terceirizar ou 'comprar' a funcionalidade on-line ou o elemento 'conectado' do dispositivo, então quem fornece esse aspecto do produto em geral também terá responsabilidades. A extensão destas variará dependendo se são um 'operador'agindo somente em seu nome ou um 'controlador'.

Entretanto, você não pode se eximir de suas obrigações de proteção de dados terceirizando o elemento 'conectado' de seu brinquedo ou dispositivo para outra pessoa. Se você fornecer um brinquedo ou um dispositivo conectado, então você precisa estar de acordo com o RGPD e seguir este código, e certificar-se de que quaisquer terceiros que você use para entregar seu produto geral também o façam.

Isto é particularmente importante, quando você está garantindo que o produto incorpora medidas de segurança adequadas para mitigar riscos, como acesso não autorizado aos dados ou '*hacking*' do dispositivo, a fim de se comunicar com a criança (por exemplo, assumir a capacidade de microfone) ou rastrear sua localização.

Antecipar e prever a utilização por múltiplos usuários de diferentes idades

Se você oferecer um dispositivo conectado, então você precisa prestar atenção no potencial de que ele possa ser usado por vários usuários de diferentes idades. Esse é o caso de dispositivos de alto-fa-

lantes interativos do *hub* doméstico, que provavelmente serão usados por vários membros da casa, incluindo crianças, e podem ser usados por visitantes da casa. Brinquedos interativos similares são frequentemente compartilhados ou podem ser usados por várias crianças ao mesmo tempo, quando brincam juntos.

Você pode fazer isso através de uma combinação de:

- certificar-se de que o serviço que você presta por padrão (o serviço que seria prestado, por exemplo, a visitantes ocasionais a um lar) é adequado para uso por todas as crianças; e
- fornecer opções de perfil de usuário para pessoas que usam o dispositivo regularmente (por exemplo, membros da família e visitantes frequentes de uma casa), com o fim de atender ao uso por adultos ou de adaptar o serviço à idade de uma determinada criança.

Fornecer informações claras sobre seu uso de dados pessoais no momento da compra e no momento da instalação

Você deve fornecer informações claras, indicando que o produto trata dados pessoais, no momento da venda e antes da instalação do dispositivo. Tanto a embalagem do produto físico, quanto o folheto do produto ou o folheto de instruções (em papel ou digital) podem conter uma indicação clara (como um ícone) de que o produto está 'conectado' e trata os dados pessoais dos usuários.

Você deve permitir que os potenciais compradores visualizem suas informações de privacidade, os termos e as condições de uso e as outras informações relevantes on-line, sem ter que comprar e configurar o dispositivo primeiro, para que eles possam tomar uma decisão informada sobre se devem ou não comprar o dispositivo em primeiro lugar.

Você também deve se preocupar com as ferramentas que fornece na intenção de facilitar a configuração do brinquedo ou do dispositivo conectado. Essa é uma oportunidade-chave para você fornecer informações sobre como seu serviço funciona, como os dados pessoais são usados e para explicar as implicações disso, especialmente se a configuração for ativada usando uma interface baseada em tela. Se o uso contínuo do dispositivo pela criança não for baseado em tela, isso é particularmente importante, pois pode limitar as formas pelas quais você pode transmitir informações à criança de forma contínua.

Encontrar maneiras de comunicar informações 'no momento' ('*just in time*'[22])

Você deve avaliar como seu dispositivo conectado funciona e como melhor comunicar informações 'bem na hora' à criança ou a seus pais. (Veja a seção deste código sobre transparência para mais detalhes sobre avisos 'bem na hora').

Por exemplo, usando mensagens de áudio de reprodução automática, permitindo apenas que as configurações padrão sejam alteradas, através do uso de um aplicativo de suporte, ou facilitando 'conversas' interativas com o usuário em modo auto-bot.

Evitar a coleta passiva de dados pessoais

Você deve providenciar recursos que deixem claro para a criança ou seus pais, quando você estiver coletando dados pessoais. Por exemplo, uma luz que acenda, quando o dispositivo estiver gravando áudio, filmando ou coletando dados pessoais de outra forma.

Se o dispositivo usa modo *stand-by* ou modo de escuta (por exemplo, ele escuta o nome que você ou a criança deu ao dispositivo, ou outra palavra ou frase-chave a ser usada, e ativa a coleta de dados quando essa palavra ou frase é usada), novamente você deve fornecer uma indicação clara de que o modo de escuta está ativo. Você não deve coletar dados pessoais no modo de escuta.

Você deve disponibilizar recursos os quais permitam que os modos de coleta ou escuta sejam facilmente desligados no próprio dispositivo (um botão 'conexão desligada'), ou através de opções de funcionalidade on-line, para que o brinquedo ou o dispositivo possa ser usado como um dispositivo não conectado, na medida do possível.

Para informações além deste código:

Guia para o RGPD - Contratos e responsabilidades entre controladores e operadores

Guia para o RGPD - Segurança

Departamento para Cultura, Mídia e Esporte Digital: Código de Práticas para a segurança do consumidor IOT (internet das coisas)

22. Providenciar informações claras sobre o que é feito com os dados pessoais em explicações mais específicas e de fácil compreensão, assim que o uso dos dados pessoais é ativado ou iniciado.

15. FERRAMENTAS ON-LINE

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

> Disponibilizar ferramentas proeminentes e acessíveis para ajudar as crianças a exercer seus direitos de proteção de dados e relatar preocupações.

O que se quer dizer com 'ferramentas on-line'?

As ferramentas on-line são mecanismos para ajudar as crianças a exercer seus direitos de forma simples e fácil, quando estão on-line. Elas podem ser usadas para ajudar as crianças a exercer seus direitos de acesso a uma cópia de seus dados pessoais, ou para fazer uma reclamação ou exercer qualquer um de seus direitos de reparação.

Por que isso é importante?

- O RGPD concede aos titulares os seguintes direitos sobre seus dados pessoais nos artigos 15 a 22:
  - O direito de acesso
  - O direito de retificação
  - O direito de eliminação dos dados
  - O direito à limitação do tratamento
  - O direito de portabilidade dos dados
  - O direito de oposição
  - Os direitos em relação a decisões automatizadas e perfilamento

O Considerando 65 estabelece que o direito à eliminação tem especial relevância para as crianças que utilizam serviços on-line:

> "...esse direito é particularmente relevante quando o titular tenha dado seu consentimento como criança e, portanto, não está plenamente consciente dos riscos envolvidos pelo tratamento, e mais tarde queira remover esses dados pessoais, especialmente na internet...".

O artigo 12, do RGPD, determina que:

> "12(1) O responsável pelo tratamento tomará as medidas adequadas para fornecer (...) qualquer comunicação prevista nos artigos 15 a 22 (...) a respeito do tratamento, de forma concisa, transparente, inteligível e

de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas, especificamente, a crianças. As informações serão prestadas por escrito ou por outros meios, inclusive, se for o caso, por meios eletrônicos (...)

(2) O responsável pelo tratamento facilitará o exercício dos direitos do titular dos dados, nos termos dos artigos 15 a 22 (...)

(3) O responsável pelo tratamento fornecerá ao titular as informações sobre as medidas tomadas, mediante pedido apresentado, nos termos dos artigos 15 a 20, sem demora injustificada, e no prazo de um mês, a contar da data de recebimento do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informará ao titular dos dados quaisquer prorrogação e motivos da demora no prazo de um mês, a contar da data de recebimento do pedido. Se o titular dos dados apresentar o pedido por meios eletrônicos, a informação é, sempre que possível, fornecida por meios eletrônicos, salvo pedido em contrário do titular."

A fim de cumprir essas disposições, você precisa encontrar formas de garantir que as crianças conheçam seus direitos e sejam capazes de exercê-los facilmente. Você tem a obrigação não apenas de permitir que as crianças exerçam seus direitos, mas de ajudá-las a fazê-lo.

Como podemos ter certeza de que cumprimos este padrão?

Para que as crianças possam exercer seus direitos, elas precisam primeiro saber que esses direitos existem e o que são.

Deixe suas ferramentas em destaque

As ferramentas que você fornece para ajudar as crianças a exercer seus direitos e relatar-lhe preocupações devem ser de fácil acesso para a criança. Portanto, você precisa dar destaque a elas em seu serviço on-line. Você deve destacar a ferramenta de relatório em seu processo de configuração e fornecer um ícone claro e facilmente identificável ou outro mecanismo de acesso, em um local de fácil identificação e acesso na tela.

Se seu serviço on-line inclui um produto físico, por exemplo, um brinquedo conectado ou um alto-falante, você pode incluir o ícone em sua embalagem, destacando as ferramentas de relatório on-line como uma característica do produto, e encontrar meios de destacar as ferramentas de relatório de forma proeminente, mesmo que o produto não seja baseado em tela.

Torne-as adequadas à idade e fáceis de usar

Suas ferramentas devem ser adequadas à idade e fáceis de usar. Portanto, você deve adaptá-las à idade da criança em questão. A tabela a seguir fornece algumas diretrizes e recomendações. Embora você esteja para desenvolver suas próprias recomendações, de acordo com o seu serviço específico, a jornada do usuário deve sempre seguir o padrão titular.

Você também deve considerar quaisquer responsabilidades adicionais assumidas perante a legislação de igualdade relevante para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

FAIXA ETÁRIA	RECOMENDAÇÕES
0-5 Pré-alfabetização e alfabetização fundamental	Fornecer ícones, avisos de áudio ou similares que até mesmo as crianças mais novas reconhecerão como significando ‘Eu não estou feliz’ ou ‘Eu preciso de ajuda’. Se esses botões forem acionados, ou se outros avisos forem respondidos, forneça material de vídeo ou áudio solicitando que a criança procure a ajuda de um dos pais ou de um adulto de confiança. Oferecer ferramentas on-line adequadas para uso dos pais.
6-9 Os principais anos do ensino fundamental	Fornecer ícones, avisos de áudio ou similares que até mesmo as crianças mais novas reconhecerão como significando ‘Eu não estou feliz’ ou ‘Eu preciso de ajuda’, e então direcione a criança para sua ferramenta on-line. Se esses botões forem acionados, ou se outros avisos forem respondidos, forneça material de vídeo ou áudio solicitando que a criança procure a ajuda de um dos pais ou de um adulto de confiança. Providenciar ferramentas on-line que as crianças poderiam, tanto usar sozinhas, como também com a ajuda de um adulto.
10-12 Anos de transição escolar	Fornecer ícones, avisos de áudio ou similares que crianças reconhecerão como significando ‘Eu não estou feliz’ ou ‘Eu preciso de ajuda’. Se esses botões forem acionados, ou se outros avisos forem respondidos, forneça material de vídeo ou áudio solicitando que a criança procure a ajuda de um dos pais ou de um adulto de confiança. Providenciar ferramentas on-line que as crianças poderiam, tanto usar sozinhas, como também com a ajuda de um adulto.
13-15 Início da adolescência	Fornecer ícones, avisos de áudio ou similares que crianças reconhecerão como significando ‘Quero manifestar uma preocupação’, ‘Quero acessar as minhas informações’ ou ‘Eu Preciso de ajuda’. Se esses botões forem acionados, ou se outros avisos forem respondidos, direcione a criança para suas ferramentas on-line e peça-lhe para obter ajuda de um dos pais ou de outra fonte confiável, se eles assim precisarem. Oferecer ferramentas on-line adequadas para o uso pela criança, sem que seja necessária a ajuda de um adulto.
16-17 Aproximando-se da maioridade	Fornecer ícones, avisos de áudio ou similares que crianças reconhecerão como significando ‘Quero manifestar uma preocupação’, ‘Quero acessar as minhas informações’ ou ‘Eu Preciso de ajuda’. Se esses botões forem acionados, ou se outros avisos forem respondidos, direcione a criança para suas ferramentas on-line e peça-lhe para obter ajuda de um dos pais ou de outra fonte confiável, se eles assim precisarem. Oferecer ferramentas on-line adequadas para o uso pela criança, sem que seja necessária a ajuda de um adulto.

Fazer com que suas ferramentas sejam específicas para os direitos que elas respaldam

Você deve adaptar suas ferramentas para atender aos direitos que as crianças têm, de acordo com o RGPD. Por exemplo:

- uma ferramenta que permita o 'download de todos os meus dados', para assegurar o direito de acesso e o direito à portabilidade dos dados;
- uma ferramenta que possibilite 'eliminar todos os meus dados' ou 'selecionar dados para eliminar', com o objetivo de assegurar o direito de eliminação;
- uma ferramenta para 'bloquear o uso dos meus dados', cumprindo, dessa forma, com os direitos de restrição ou objeção ao tratamento; e
- uma ferramenta de 'correção', para assegurar o direito à retificação.

Utilizadas juntamente com a configuração de privacidade, essas ferramentas devem ajudar a dar às crianças o controle sobre seus dados pessoais.

Incluir mecanismos para acompanhar o andamento e se comunicar com você

Suas ferramentas on-line podem incluir meios para que a criança ou seus pais possam acompanhar o progresso de sua reclamação ou sua solicitação e se comunicar com você sobre o que está acontecendo.

Você deve fornecer informações sobre seus prazos para responder às solicitações das crianças, a fim de exercer seus direitos, e deve lidar com todas as solicitações dentro dos prazos estabelecidos no Artigo 12(3), do RGPD.

Você deve ter mecanismos para as crianças indicarem que elas acreditam que sua reclamação ou seu pedido é urgente e por quê, e você deve considerar ativamente qualquer informação que elas forneçam a esse respeito e estabelecer prioridades em conformidade. Você deve ter procedimentos em vigor para tomar medidas rápidas quando for informado acerca de problemas de proteção contínuos.

Para informações além deste código:

Guia para o RGPD - direitos individuais

GOVERNANÇA E RESPONSABILIDADE (*ACCOUNTABILITY*)

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

De forma resumida:

Você deve criar sistemas para apoiar e demonstrar sua conformidade com a legislação de proteção de dados e a conformidade com este código. Aqueles devem incluir a implementação de um programa de responsabilidade, ter políticas adequadas de proteção de dados em vigor, proporcionar um treinamento adequado para seu pessoal e manter registros adequados de suas atividades de tratamento.

De forma mais detalhada:

- O que se quer dizer com 'governança e responsabilidade'?
- Por que isso é importante?
- O que precisamos fazer?
- E quanto à certificação?

O que se quer dizer com 'governança e responsabilidade'?

Governança e responsabilidade significam ter sistemas implementados para respaldar e demonstrar o cumprimento da legislação de proteção de dados e deste código.

Por que isso é importante?

É importante porque é um veículo para você estabelecer a conformidade como uma atividade sustentável a longo prazo em toda a sua empresa. É um conceito global que pode funcionar em todas as jurisdições e permitir diferentes abordagens, sob diferentes leis, para se encaixar. É mais bem-sucedido quando apoiado pela liderança em nível de diretoria.

O artigo 24(1), do RGPD, prevê que:

> "24(1) Levando em conta a natureza, o escopo, o contexto e os objetivos do tratamento, bem como os riscos aos direitos e às liberdades das pessoas físicas, cujas probabilidade e severidade podem variar, o controlador deverá implementar medidas técnicas e organizacionais adequadas para garantir e poder demonstrar que o tratamento é realizado de acordo com este regulamento. Essas medidas devem ser revistas e atualizadas, conforme necessário.

O artigo 5(2), do RGPD, estabelece que você precisa ser capaz de demonstrar sua conformidade com os princípios de proteção de dados:

> "O controlador será responsável e capaz de demonstrar o cumprimento do parágrafo 1 (responsabilidade)".

O que devemos fazer?

Implementar um programa de responsabilidade

Você deve implementar um programa de responsabilidade para cumprir, efetivamente, os parâmetros deste código. Isso pode ser adaptado ao tamanho e aos recursos da sua empresa ou da sua organização e aos riscos para as crianças inerentes ao seu serviço on-line. Deve ser conduzido pelo seu DPO, se você tiver nomeado um, e supervisionado pela alta administração em nível de diretoria, se sua empresa estiver estruturada dessa forma. Para empresas menores, que podem não ter essas estruturas formais, ainda é importante garantir que a privacidade das crianças seja compreendida pelo pessoal-chave e seja vista como uma prioridade empresarial importante e uma medida-chave de responsabilidade.

Você deve avaliar e revisar o programa de forma contínua, incorporando mudanças para refletir as transformações do ambiente de privacidade das crianças.

Você deve relatar de acordo com os parâmetros deste código em qualquer relatório de responsabilidade interno ou externo, introduzindo KPIs (indicadores-chave de desempenho) sobre a privacidade das crianças para apoiar isso, conforme apropriado.

Dispor de políticas para apoiar e demonstrar sua conformidade com a legislação de proteção de dados

Você deve ter políticas (proporcionais ao tamanho de sua organização) que registrem como sua organização assegura a aderência a este código e às exigências do RGPD e do RPCE. Para organizações maiores, essas devem incluir mecanismos apropriados de relatórios em nível de diretoria e mecanismos para assegurar o fornecimento de recursos adequados aos projetos relevantes.

Sobretudo, você deve assegurar que suas políticas englobem suas obrigações nos termos do Artigo 30(1), para manter um registro de suas atividades de tratamento.

Capacitar sua equipe de funcionários em questões de proteção de dados

Para atender às exigências do RGPD, qualquer funcionário envolvido no projeto de seu SSI precisa entender quais são essas exigências e como esperamos que elas sejam atendidas. Portanto, você deve certificar-se de que seu pessoal receba treinamento apropriado em proteção de dados e esteja ciente das disposições do RGPD e deste código.

Manter registros adequados

Nos termos do artigo 30(1), do RGPD, você deve manter os seguintes registros de suas atividades de tratamento:

- o nome e os contatos de sua organização e, no que aplicável, de qualquer outro responsável pelo tratamento e do encarregado da proteção de dados (DPO);
- as finalidades do tratamento dos dados;
- a descrição das categorias de titulares de dados e dos tipos de dados pessoais;
- as categorias de destinatários de dados pessoais;
- os detalhes sobre as suas transferências de dados pessoais para países terceiros, incluindo a documentação dos mecanismos de proteção em prática;
- os prazos de guarda do dado pessoal;
- e uma descrição de suas medidas de segurança técnica e organizacional.

No contexto da prestação de um serviço on-line, essa regra se aplica a você, independentemente do tamanho de sua organização. Isso porque a Autoridade considera que, dada a vulnerabilidade das crianças e os riscos inerentes a elas ao estarem on-line, qualquer tratamento desse tipo é suscetível de resultar em um risco para os direitos e as liberdades das crianças.

Em nosso site, dispomos de modelos que você pode utilizar para registrar esses detalhes.

Você também deve manter um registro de seu RIPD. Trata-se de um documento-chave que você pode utilizar para demonstrar que considerou adequadamente e mitigou os riscos decorrentes de seu tratamento de dados pessoais de crianças. Ele deve ajudá-lo a demonstrar seu raciocínio e suas decisões sobre:

- se é provável que as crianças tenham acesso ao seu serviço on-line;
- quais as idades das crianças que, provavelmente, terão acesso ao seu serviço on-line;
- e que medidas você tomou para cumprir com este código.

Esteja preparado para demonstrar sua conformidade com este código

Você deve estar preparado para demonstrar sua conformidade com este código à ICO, se lhe pedirmos que assim o faça. Você pode fazer isso, primeiramente nos fornecendo cópias de seu RIPD, suas políticas relevantes, seus registros de treinamento e seus registros de atividades de tratamento. Você também pode precisar fornecer provas de como implementou as disposições do código em seu serviço on-line na prática. Por exemplo, mostrando-nos seus avisos de privacidade, ou explicando ou demonstrando suas configurações padrão, ferramentas on-line, processos de reclamação e abordagem ao perfilamento.

E quanto à certificação?

O Artigo 42 do RGPD prevê um mecanismo para o estabelecimento de certificação e de selo de proteção de dados, através do qual os controladores de dados poderiam demonstrar sua conformidade com o RGPD.

Isso beneficiaria as crianças e seus pais na tomada de decisões sobre quais serviços on-line usar (ou permitir que seus filhos usem), sem ter que avaliar a conformidade e a prática do próprio provedor de serviços on-line.

Também o beneficiaria como fornecedor de um serviço on-line, para dar garantia aos seus clientes e clientes potenciais de sua conformidade com a proteção de dados, aumentando assim a confiança do consumidor no serviço on-line e na marca.

Quando esses sistemas estiverem disponíveis e oferecerem certificação de adesão a este código, você poderá utilizá-los para demonstrar sua conformidade, de acordo com o Artigo 24(1), do RGPD.

Para informações além deste código:

Guia de responsabilidade e governança, de acordo com o RGPD

Modelo de documentação para os controladores

Modelo de documentação para os operadores

CUMPRIMENTO DESTE CÓDIGO (*ENFORCEMENT*)

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

De forma resumida:

A ICO sustenta os direitos de informação no interesse público. Os dados relativos às crianças recebem proteção especial no RGPD e são uma prioridade regulatória para a ICO. A conformidade com os parâmetros estabelecidos neste código será uma medida fundamental para que você cumpra com as leis de proteção de dados.

Monitoraremos a conformidade com este código através de uma série de auditorias proativas, consideraremos reclamações e tomaremos as medidas apropriadas para fazer cumprir com os parâmetros de proteção de dados subjacentes, tudo sujeito à lei aplicável e de acordo com nossa Política de Ação Regulatória. Para assegurar uma regulamentação proporcional e eficaz, direcionaremos nossos poderes mais significativos, concentrando-nos em organizações e indivíduos suspeitos de má conduta repetida ou deliberada ou de falha grave no cumprimento da lei. Se você não seguir este código, pode ter dificuldade em demonstrar que seu tratamento é leal e em conformidade com o RGPD ou o RPCE.

Temos diversas possibilidades de ação em caso de violação do RGPD ou do RPCE, inclusive quando os dados pessoais de uma criança tenham sido processados em violação às disposições relevantes dessas leis. Isso inclui o poder de emitir advertências, reprimendas, ordens de *stop-now* (mecanismo regulatório) e multas.

De forma mais detalhada:

- Qual é o papel da ICO?
- Como a ICO irá monitorar o cumprimento?
- Como a ICO irá lidar com as reclamações?
- Quais são os poderes de execução da ICO?

Qual é o papel da ICO?

A ICO é a autoridade supervisora independente para a proteção de dados no Reino Unido.

Nossa missão é defender os direitos de informação para o público na era digital. Nossa visão para a proteção de dados é aumentar a confiança

que o público tem nas organizações que tratam dados pessoais. Oferecemos aconselhamento e orientação, promovemos boas práticas, monitoramos e investigamos relatórios de violação, monitoramos o cumprimento, realizamos auditorias e visitas consultivas, recebemos reclamações e tomamos medidas de execução, quando apropriado. Nossos poderes de *enforcement* estão definidos na parte 6, da DPA 2018.

Nosso foco é estar em conformidade com a legislação de proteção de dados no Reino Unido. Em particular, para assegurar que as proteções previstas para os dados das crianças sejam cumpridas.

Quando as disposições deste código se sobrepuserem a outros regulamentos, trabalharemos em conjunto para assegurar uma resposta consistente e coordenada.

Como a ICO irá monitorar a conformidade?

Os principais objetivos de nossa Política de Ação Regulatória incluem:

> "Ser proativo na identificação e na mitigação de riscos novos ou emergentes, decorrentes de mudanças tecnológicas e da sociedade" e,
>
> "Ser eficaz, proporcional, dissuasivo e consistente em nossa aplicação de sanções, visando aos nossos poderes mais significativos (i) para organizações e indivíduos suspeitos de má conduta repetida ou intencional ou de falhas graves, na tomada de medidas adequadas para proteger dados pessoais, e (ii) quando a ação regulatória formal serve como um importante dissuasor, para aqueles que correm o risco de não estar em conformidade com a lei".

Também consideramos o uso dos dados das crianças como uma prioridade regulatória.

Monitoraremos a conformidade com este código usando toda a gama de medidas disponíveis, desde a coleta de informações, até a utilização de nossos poderes de auditoria ou avaliação para entender um problema, passando pela investigação e pela ação regulatória, quando apropriado e proporcional.

Nossa abordagem é incentivar a conformidade. Quando encontramos problemas, tomamos medidas regulatórias justas, proporcionais e oportunas, com o objetivo de garantir que os direitos de informação dos indivíduos sejam devidamente protegidos. Levaremos em conta o tamanho e os recursos da organização em questão, a disponibilidade de soluções tecnológicas no mercado e os riscos para as crianças que são inerentes ao tratamento. Tomaremos uma abordagem proporcional e responsável, concentrando-nos nas áreas com maior potencial de dano e selecionando a ferramenta regulatória mais adequada.

Como a ICO lida com as reclamações?

Se alguém levantar uma preocupação conosco sobre sua conformidade com este código ou a forma como você tratou os dados pessoais de uma criança, no contexto de um serviço on-line relevante, registraremos e consideraremos essa reclamação.

Levaremos este código em consideração, juntamente com outras legislações relevantes, ao considerar se você cumpriu com o RGPD ou o RPCE. Especificamente, levaremos o código em consideração, quando considerarmos questões de lealdade, licitude, transparência e responsabilidade.

Avaliaremos sua resposta inicial à reclamação e poderemos entrar em contato com você para fazer algumas perguntas e dar-lhe uma oportunidade adicional de explicar sua posição. Também podemos solicitar detalhes de suas políticas e seus procedimentos, seu RIPD e outras documentações relevantes. Todavia, esperamos que você seja responsável pelo cumprimento de suas obrigações, nos termos do RGPD e do RPCE, portanto, você deve certificar-se de que, quando inicialmente responder a reclamações de indivíduos, o faça com uma explicação completa e detalhada sobre como você utiliza seus dados pessoais e como você está em conformidade.

Se considerarmos que você falhou (ou está falhando) no cumprimento do RGPD ou do RPCE, temos o poder de tomar medidas coercitivas. Isso pode exigir que você tome medidas para colocar suas operações em conformidade, ou podemos decidir multá-lo. Ou ambos.

Quais são os poderes de execução da ICO?

Temos diferentes formas de agir, em caso de violação do RGPD ou do RPCE, inclusive quando se trata de dados pessoais de uma criança. Temos o dever estatutário de levar em conta as disposições deste código, ao fazer cumprir o RGPD e o RPCE.

Sem prejuízo das especificidades da legislação aplicável, como o Regulamento de Comércio Eletrônico de 2002, as ferramentas à nossa disposição incluem avisos de avaliação, advertências, repreensões, avisos de execução e notificações de penalidades (multas administrativas). Para violações graves dos princípios de proteção de dados, temos o poder de emitir multas de até 20 milhões de euros (ou £17,5 milhões, quando o RGPD do Reino Unido entrar em vigor) ou de 4% do seu faturamento anual mundial, o que for maior.

De acordo com nossa política, consideramos que o interesse público em proteger as crianças on-line é um fator significativo, que pesa na

balança ao considerar o tipo de ação regulatória. Isso significa que, quando virmos danos ou potenciais danos às crianças, provavelmente tomaremos medidas mais severas contra uma empresa do que as que seriam tomadas para outros tipos de dados pessoais. No entanto, levaremos em conta o tamanho e os recursos da organização em questão, a disponibilidade de soluções tecnológicas no mercado e os riscos específicos para as crianças que são inerentes ao tratamento. Também levaremos em conta os esforços feitos para cumprir com as disposições deste código.

Para informações além deste código:

O que fazemos

Faça uma reclamação

Que medidas a ICO pode tomar para fazer cumprir o RPCE?

Política de Ação Regulatória

GLOSSÁRIO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

O presente glossário está incluído como um ponto de referência rápido para os principais termos e abreviaturas de proteção de dados utilizados neste código. Ele inclui links para leituras adicionais e outros recursos que não fazem parte deste código, mas podem fornecer contexto útil e uma orientação mais detalhada.

ASA	A autoridade de Normas Publicitárias. Acessar: https://www.asa.org.uk/
CÓDIGO CAP	O Código de Não-Transmissão Publicitária do Reino Unido & Marketing Promocional Direto *(The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing*). Acessar: https://www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html
CRIANÇA	Uma pessoa com menos de 18 anos de idade, conforme definido no CNUDC.
AUTORIDADE COMPETENTE	A autoridade pública listada no cronograma 7, da DPA 2018, ou qualquer outra organização ou pessoa com funções legais de aplicação da lei. Para mais informações, consulte nosso guia: Guia para o tratamento da Aplicação da Lei.
CONSENTIMENTO	Uma indicação livre, específica, informada e inequívoca da vontade da pessoa em questão, pela qual ele ou ela, por uma declaração ou por uma clara ação afirmativa, manifesta a concordância com o tratamento de dados pessoais. Para maiores informações, consulte nossa orientação separada sobre consentimento.
CONTROLADOR	A pessoa (geralmente uma organização) que decide como e por que coletar e utilizar os dados. Para mais informações, consulte nossa orientação separada sobre controladores e processadores.
DPA 2018	A Lei de Proteção de Dados de 2018. Para mais informações, consulte nossa seção: Introdução à proteção de dados.
RIPD	(RIPD) Avaliação do impacto da proteção de dados. Para mais informações, consulte nossa seção sobre RIPDs.
RGPD	O Regulamento Geral de Proteção de Dados (UE) 2016/679, conforme emendado e incorporado à legislação britânica. Para mais informações, consulte nosso Guia de Proteção de Dados à parte. Quando o Reino Unido deixar a UE (ou ao final de qualquer período de implementação acordado, se sairmos com um acordo), você deverá ler as referências ao RGPD, neste código, como referências ao RGPD do Reino Unido.
ISS	Serviço da sociedade da informação, conforme definido na Diretiva (UE) 2015/1535 e incorporado ao RGPD (qualquer serviço normalmente prestado mediante remuneração, à distância, por meios eletrônicos e a pedido individual de um destinatário).

ONE-STOP-SHOP	O "*one-stop-shop*" significa que você, geralmente, pode lidar com uma única autoridade supervisora europeia tomando medidas em nome das outras autoridades supervisoras europeias. Ele evita que você tenha que lidar com ações regulatórias e de fiscalização, de cada autoridade supervisora, em cada estado da EEA, e da EU, onde os indivíduos são afetados. Para mais informações, consulte as diretrizes da CEPD sobre a autoridade supervisora líder.
RPCE	Os Regulamentos de Privacidade e Comunicações Eletrônicas (Diretiva da CE) de 2003. Para mais informações, acesse: Guia ao RPCE.
PEGI (PAN EUROPEAN GAME INFORMATION)	Informação Pan-Europeia de Jogos (PEGI) é um sistema europeu de classificação de conteúdo de jogos eletrônicos e outros programas de entretenimento para computador ou outras plataformas. Para mais informações, acessar: https://pegi.info/.
OPERADOR	Uma pessoa (geralmente uma organização) que trata os dados pessoais em nome de um controlador. Para mais informações, consulte nossa orientação separada sobre controladores e operadores.
RGPD UK	A versão britânica do RGPD, conforme emendada e incorporada à legislação britânica, depois que o Reino Unido deixar a EU, pela Lei da União Europeia (*Withdrawal*) de 2018 e pelos Regulamentos de Saída associados. O governo publicou um calendário (*Keeling Schedule*) para o RGPD do Reino Unido, que indica as emendas planejadas.
CNUDC	A Convenção das Nações Unidas sobre os Direitos da Criança de 1989.

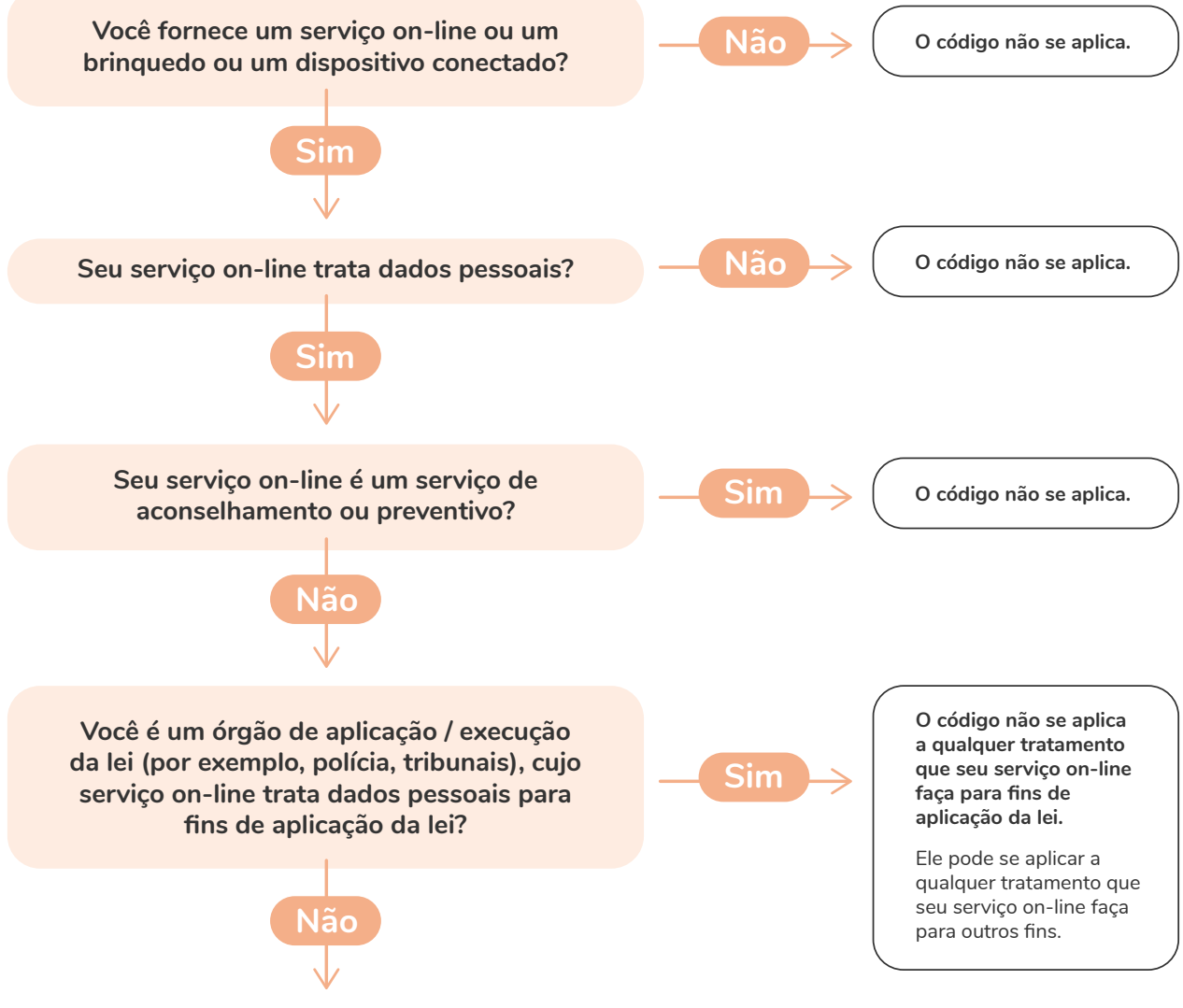
ANEXO A: SERVIÇOS COBERTOS PELO DIAGRAMA DE FLUXO DO CÓDIGO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Este fluxograma estabelece as perguntas que você precisará responder, caso tenha dúvidas se o seu serviço on-line está coberto pelo código.

No entanto, como ponto de partida, você deve observar que esperamos que a grande maioria dos serviços on-line utilizados por crianças estejam contemplados e aqueles que não estão contemplados sejam excepcionais.

Os serviços que estão fora do escopo tendem a fazê-lo por razões técnicas legais (por exemplo, a definição de um SSI como derivado, conforme a Diretiva EU 2015/1535), portanto, se você acha que pode estar fora do escopo, então você poderá se beneficiar, ao receber seu próprio aconselhamento jurídico para apoiar ou confirmar isso.



Seu serviço on-line é o tipo de serviço que, normalmente, é fornecido ou financiado em uma base comercial (mesmo que o financiamento não seja fornecido pelo usuário final)?

Não → **O código não se aplica.**

Sim ↓

Seu serviço on-line é um serviço de "transmissão geral" (um serviço que transmite transmissões de rádio ou TV para uma audiência geral, de acordo com uma programação ou horário definido)?

Sim → **O código não se aplica aos seus serviços de "transmissão geral".**

Se você também fornece serviços de transmissão 'sob demanda', então o código pode se aplica a esses serviços.

Não ↓

Seu serviço on-line só fornece informações sobre um negócio do 'mundo real' (sem permitir que os clientes comprem produtos ou acessem serviços específicos on-line)?

Sim → **O código não se aplica.**

Não ↓

Seu serviço é um serviço de telefonia de voz 'tradicional', em oposição a um serviço de chamadas de voz pela Internet ou VOIP (*Voice Over Internet Protocol*)?

Não → **O código não se aplica.**

Não ↓

É provável que seu serviço on-line seja acessado por crianças? (Isso dependerá da probabilidade de o conteúdo e o design de seu serviço ser atraente para as crianças e de quaisquer medidas que você possa ter para restringir ou desencorajar o acesso delas ao seu serviço).

Não → **O código não se aplica.**

Sim ↓

Você tem um escritório, base ou outro 'estabelecimento' no Reino Unido, e seu serviço on-line trata dados pessoais no contexto desse estabelecimento?

Não → **O código se aplica ao seu serviço, se o seu serviço atender aos seguintes critérios:**

- você oferece seu serviço on-line aos usuários do Reino Unido ou monitora o comportamento dos usuários do Reino Unido; e
- (até o Reino Unido sair da UE) você não tem uma base de escritório ou outro estabelecimento em outro lugar dentro do EEA (Espaço Econômico Europeu).

Caso contrário, o código não se aplica.

Sim ↓

O código se aplica ao seu serviço.

ANEXO B: IDADE E ESTÁGIOS DE DESENVOLVIMENTO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

As crianças são indivíduos, e as faixas etárias não são um guia perfeito para os interesses, as necessidades e desenvolvimento progressivo de uma criança individual. Contudo, você pode usar as faixas etárias como um guia para a capacidade, as habilidades e os comportamentos que se pode esperar de uma criança em cada estágio de seu desenvolvimento, para ajudá-lo a avaliar o que é adequado para crianças, de uma maneira geral, daquela idade.

Este anexo fornece algumas orientações sobre considerações-chave relevantes em diferentes idades. Foi desenvolvido com base nas respostas ao pedido da ICO de provas, sobre o Código *Design* Apropriado à idade, pesquisa financiada por Sonia Livingstone, na Escola de Economia e Ciência Política de Londres (LSE), e com base nas seguintes fontes:

- Relatório UKCCIS Educação para um mundo conectado
- Relatório UKCCIS sobre atividades on-line, riscos e segurança das crianças
- Guia UKCCIS de Segurança Infantil On-line
- Relatório da Comissão de Criança da Inglaterra sobre a vida à base de “curtidas”
- Relatório da Fundação 5Rights sobre uma Infância Digital
- Relatório de Revelação da Realidade Rumo a um futuro digital melhor Informando o Código de *Design* Apropriado à Idade

Crianças com deficiências podem ter necessidades adicionais e você deve considerar quaisquer responsabilidades adicionais assumidas perante a legislação de igualdade relevante para a Inglaterra, a Escócia, o País de Gales e a Irlanda do Norte.

FAIXA ETÁRIA / ESTÁGIO DE DENVOLVIMENTO	PRINCIPAIS CONSIDERAÇÕES
0-5 Pré-alfabetização e alfabetização fundamental	Há relativamente poucas evidências sobre a compreensão do ambiente digital das crianças nesta faixa etária, particularmente na faixa de 0-3 anos de idade. Porém, evidências anedóticas sugerem que um número significativo de crianças está on-line desde as primeiras idades e que quaisquer compreensão e consciência dos riscos on-line por crianças, dentro desta faixa etária, são muito limitadas. Entre 3 e 5 anos de idade, as crianças começam a desenvolver a capacidade de 'se colocar no lugar dos outros', mas são facilmente enganadas pelas aparências. Elas estão desenvolvendo amizades, embora a pressão dos colegas seja relativamente baixa e a orientação ou a influência dos pais ou da família seja fundamental. Elas estão aprendendo a seguir regras claras e simples, mas é improvável que tenham a capacidade cognitiva de compreender ou de seguir regras ou instruções com mais nuances, ou de tomar qualquer outra coisa que não seja a mais simples das decisões. Elas têm capacidade limitada de autocontrole ou de administrar seu próprio tempo on-line. Elas estão predominantemente envolvidas em atividades guiadas por adultos, brincando dentro de ambientes 'protegidos' ou assistindo a transmissões de vídeo. Crianças nesta faixa etária são menos propensas que crianças mais velhas a terem seu próprio dispositivo, embora um número significativo de crianças bem novas já conte com um dispositivo próprio e, muitas vezes, brinque com os dispositivos de seus pais, que podem ou não ser configurados com perfis específicos de crianças. Elas podem usar brinquedos conectados (como brinquedos de pelúcia falantes ou bonecos) e podem imitar o uso de dispositivos ativados por voz dos pais, como os '*hubs* domésticos'. As crianças dentro desta faixa etária são pré-alfabetizadas ou estão nos estágios iniciais de alfabetização, portanto, as informações baseadas em texto têm um uso muito limitado na comunicação com elas. Crianças britânicas nesta faixa etária não podem dar seu próprio consentimento para o tratamento de seus dados pessoais, no contexto de um serviço on-line oferecido diretamente a uma criança (em virtude do Artigo 8(1), do RGPD, e s9 da DPA 2018). Portanto, se você deseja confiar no consentimento, como base legal para o tratamento de seus dados pessoais, você precisa do consentimento dos pais.

6-9 Os principais anos da escola fundamental	As crianças nesta faixa etária são mais propensas a ter seu próprio dispositivo (como um tablet), embora o uso dos dispositivos dos pais ainda seja comum. Eles estão usando cada vez mais dispositivos de forma independente, com ou sem o benefício de perfis específicos de crianças. Brinquedos conectados são populares e podem se envolver entusiasticamente com dispositivos ativados por voz, como os "*hubs* domésticos". As crianças nesta faixa etária, geralmente, preferem jogos on-line e atividades baseadas na criatividade, e os serviços de *streaming* de vídeo continuam populares. As crianças podem ter contato com redes sociais, seja através dos aspectos sociais dos jogos on-line, seja através das contas de rede social de seus pais ou da criação de suas próprias contas de rede social. Elas podem se relacionar e ser influenciadas por internautas, particularmente aqueles dentro de uma faixa etária semelhante. É provável que elas estejam absorvendo mensagens da escola sobre segurança on-line e o ambiente digital e estejam desenvolvendo uma compreensão básica dos conceitos de privacidade e alguns dos riscos on-line mais óbvios. Porém, é improvável que elas tenham uma compreensão clara das muitas maneiras pelas quais seus dados pessoais podem ser usados ou de quaisquer riscos menos diretos ou óbvios aos quais seus comportamentos on-line possam expô-las. A necessidade de integrar-se com seu grupo de colegas torna-se mais importante, de forma que elas possam ser mais suscetíveis à pressão dos colegas. No entanto, o lar e a família ainda tendem a ser os mais fortes influenciadores. Elas ainda tendem a obedecer a mensagens ou regras claras de casa e da escola, contudo, se os riscos não forem explicados claramente, elas podem preencher a lacuna com suas próprias explicações ou inventar estratégias de proteção que não são tão eficazes, quanto pensam que são. Os níveis de alfabetização podem variar consideravelmente e a capacidade ou a disposição de se envolver com materiais escritos não pode ser assumida. Crianças britânicas nesta faixa etária não podem fornecer seu próprio consentimento para o tratamento de seus dados pessoais, no contexto de um serviço on-line oferecido diretamente a uma criança (em virtude do Artigo 8(1), do RGPD, e s9 da DPA 2018). Portanto, se você deseja confiar no consentimento como base legal para o tratamento de seus dados pessoais, você precisa do consentimento dos pais.

10-12 Anos de transição escolar	Trata-se de uma faixa etária chave na qual a atividade on-line das crianças provavelmente mudará significativamente. A transição, ou a transição antecipada, da escola primária para o ensino médio, significa que é muito mais provável que as crianças tenham seu próprio dispositivo pessoal (smartphones predominantemente). Também é provável que haja uma mudança no uso do ambiente on-line para explorar e desenvolver a autoidentidade e os relacionamentos, para expandir e permanecer em contato com seu grupo de colegas e para 'encaixar-se' socialmente. Isso pode levar a um maior uso de funções ou serviços de redes sociais por crianças dentro desta faixa etária, a uma maior suscetibilidade à pressão dos colegas, à estigmatização e aos 'influenciadores' on-line, e ao aumento dos comportamentos de tomada de risco. A autoestima pode cair à medida que as crianças se comparam a outras e se esforçam para apresentar uma versão aceitável de si mesmas on-line, e o 'medo de ficar de fora' pode se tornar uma preocupação. Os jogos on-line e os serviços de *streaming* de vídeo e música também são populares. As crianças podem se sentir pressionadas a jogar jogos on-line, quando seus amigos estão jogando, novamente por medo de 'ficarem de fora', por medo de exclusão. As atitudes em relação às regras dos pais, à autoridade e ao envolvimento em sua atividade on-line podem variar consideravelmente, com algumas crianças aceitando relativamente isso e outras buscando níveis mais altos de autonomia. Todavia, os pais e a família ainda tendem a ser a principal fonte de influência para as crianças nesta faixa etária. As crianças nesta faixa etária estão se encaminhando para uma forma de pensar mais adulta, mas podem ter capacidade limitada de pensar além das consequências imediatas, ser particularmente suscetíveis a sistemas baseados em recompensas e tender a comportamentos impulsivos. Os pais ou outros apoios, portanto, ainda tendem a ser necessários, se não sempre desejados. No entanto, pode precisar ser oferecido ou incentivado de uma forma menos diretiva do que para crianças menores. Crianças nesta faixa etária estão desenvolvendo uma melhor compreensão de como o ambiente on-line funciona, mas ainda é pouco provável que tenham conhecimento de usos menos óbvios de seus dados pessoais. Embora as crianças nesta faixa etária, provavelmente, tenham habilidades de alfabetização mais desenvolvidas, elas ainda podem preferir mídias como conteúdo de vídeo. 12 é a idade em que, sob o s208 da DPA 2018, presume-se que as crianças na Escócia (a menos que o contrário seja demonstrado) tenham idade e maturidade suficientes para ter uma compreensão geral do que significa exercer seus direitos de proteção de dados. Não existe nenhuma disposição desse tipo para crianças no resto do Reino Unido, embora isso possa ser considerado um ponto de referência útil. Crianças britânicas nessa faixa etária não podem dar seu próprio consentimento para o tratamento de seus dados pessoais, no contexto de um serviço on-line oferecido, diretamente, a uma criança (em virtude do Artigo 8(1), do RGPD, e s9, da DPA 2018). Portanto, se você deseja confiar no consentimento, como base legal para o tratamento de seus dados pessoais, você precisa do consentimento dos pais.

13-15 Início da adolescência	Neste intervalo etário, a necessidade de identificação com seu próprio grupo de colegas e a exploração da identidade e dos relacionamentos aumenta ainda mais, e é provável que as crianças busquem maiores níveis de independência e autonomia. Elas podem rejeitar ou se distanciar dos valores de seus pais ou procurar ostentar ativamente as regras dos pais ou on-line. O uso de novos serviços que os pais não conhecem ou não usam é popular, assim como o uso de linguagem que os pais podem não entender facilmente. No entanto, apesar disso, a família continua sendo uma influência-chave sobre as crianças dentro desta faixa etária. O uso das funções e das aplicações das mídias sociais é amplamente difundido, embora jogos e serviços de *streaming* de vídeo e música também sejam populares. Novamente, as crianças podem procurar imitar os 'influenciadores' ou os vloggers on-line nesta fase de seu desenvolvimento. Crianças desta idade ainda podem procurar ajuda dos pais, caso encontrem problemas on-line, mas alguns podem estar relutantes em fazê-lo, devido à preocupação com a reação de seus pais à sua atividade on-line. Em termos de desenvolvimento, eles podem tender ao pensamento idealizado ou polarizado e ser suscetíveis à comparação negativa de si mesmos com outros. Eles podem superestimar sua própria capacidade de lidar com riscos e desafios decorrentes do comportamento e relacionamentos on-line e podem se beneficiar da sinalização para, inclusive, mas sem se limitar a, fontes de apoio dos pais. É provável que as habilidades de alfabetização sejam mais desenvolvidas, mas elas ainda podem se beneficiar de uma escolha de mídia. 13 é a idade em que as crianças no Reino Unido são capazes de fornecer seu próprio consentimento para o tratamento, se você estiver confiando no consentimento como base legal para o tratamento no contexto de oferecer um serviço on-line diretamente a uma criança (em virtude do Artigo 8(1), do RGPD, e s9, da DPA 2018).
16-17 Aproximando-se da maioridade	Nesta idade, muitas crianças já desenvolveram habilidades on-line razoavelmente robustas, estratégias de enfrentamento e resiliência. Todavia, elas ainda estão se desenvolvendo cognitiva e emocionalmente e não se deve esperar que tenham as mesmas resiliência, experiência ou apreciação das consequências a longo prazo, de suas ações on-line, que os adultos podem ter. Os conhecimentos e as capacidades técnicas podem ser mais desenvolvidos do que sua alfabetização emocional ou sua capacidade de lidar com relações pessoais complexas. Sua capacidade de pensar a longo prazo ainda está se desenvolvendo e eles ainda podem tender a assumir riscos ou comportamentos impulsivos e ser suscetíveis a sistemas baseados em recompensas. É muito mais provável que o apoio dos pais seja visto como uma opção que eles podem ou não querer usar, em vez de ser a opção preferida ou única, e eles esperam um nível razoável de autonomia. A sinalização para outras fontes de apoio, além do apoio dos pais, é importante. Em virtude do Artigo 8(1), do RGPD, e s9, da DPA 2018, se você estiver confiando no consentimento, como base legal para o tratamento no contexto de oferecer um serviço on-line diretamente a uma criança, as crianças britânicas nesta faixa etária podem fornecer seu próprio consentimento para o tratamento de seus dados pessoais.

ANEXO C: BASES LEGAIS PARA O TRATAMENTO

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

A orientação, neste anexo, não está vinculada a uma norma específica no código, contudo, se você fornece um serviço on-line para crianças, ele o ajudará a cumprir suas obrigações de legalidade nos termos do RGPD e da DPA 2018.

- O que é uma base legal para o tratamento?
- Que base legal podemos usar para nosso tratamento essencial (*core*)?
- Que base legal podemos usar para o tratamento 'não essencial'?
- Quando temos que obter o consentimento dos pais?
- E os dados de categorias especiais?

O que é uma base legal para o tratamento?

Você deve ter uma base legal válida para cada uma de suas atividades de tratamento. O artigo 6, do RGPD, estabelece seis bases legais em potencial:

- **Consentimento:** o indivíduo deu um consentimento válido para que você possa tratar seus dados pessoais para um propósito específico.
- **Contrato:** o tratamento é necessário para executar um contrato que você tem com o indivíduo, ou porque lhe pediram que tomasse medidas específicas, antes de firmar um contrato.
- **Obrigação legal:** o tratamento é necessário para que você cumpra a lei (não incluindo as obrigações contratuais).
- **Interesses vitais:** o tratamento é necessário para proteger a vida de alguém.
- **Função pública:** o tratamento é necessário para que você desempenhe uma tarefa de interesse público ou para suas funções oficiais, e a tarefa ou a função tem uma base clara na lei.
- **Interesses legítimos:** o tratamento é necessário para seus interesses legítimos ou os interesses legítimos de terceiros, a menos que haja um bom motivo para proteger os dados pessoais do indivíduo que se sobreponha a esses interesses legítimos – em

particular quando se trata de uma criança. (Isso não pode se aplicar, se você for uma autoridade pública que desempenha suas tarefas oficiais).

Cabe a você decidir qual base legal para o tratamento é mais apropriada para seu tratamento e demonstrar que ela se aplica. Isso depende de seus propósitos específicos e do contexto do tratamento. Na prática, é provável que você tenha mais de um propósito, caso em que você poderá ter mais de uma base para o tratamento.

Você deve considerar isso separadamente para cada atividade de tratamento distinta, pensando no que você quer fazer com os dados pessoais que está coletando e por que, e levando em conta como isso é essencial para a prestação de seu serviço on-line.

Para informações além deste código:

Base legal para o tratamento

Ferramenta de orientação interativa sobre bases legais

Que base legal podemos usar para nosso tratamento essencial (core)?

Por 'tratamento essencial', entendemos o tratamento que é integral ao fornecimento de seu serviço essencial – em outras palavras, você precisa tratar os dados dessa forma, a fim de realmente entregar os elementos do serviço que o indivíduo se inscreveu. Isso não inclui o tratamento para fins comerciais mais amplos (por exemplo, para marketing, para melhoria do serviço ou como parte de um modelo de financiamento indireto).

Para esse tipo de tratamento, você poderia considerar:

- **Contrato:** a base mais óbvia é 'necessária para a execução de um contrato'. Contudo, se você quiser depender desta base, você precisa ter certeza de que a criança tem a capacidade legal para celebrar um contrato. Se a criança não for competente para firmar o contrato, então o contrato é anulável. Se o contrato for anulado, então esta base para o tratamento não será válida.
- **Interesses legítimos:** alternativamente, você pode considerar interesses legítimos (a menos que você seja uma autoridade pública que desempenhe suas funções). Se você optar por basear-se em interesses legítimos, você tem uma responsabilidade particular de proteger as crianças dos riscos que elas podem não apreciar plenamente e das consequências que elas podem não prever.

Você deve assegurar que seus interesses sejam adequadamente protegidos e que haja salvaguardas apropriadas. Você precisa dar peso extra aos seus interesses e precisa de um interesse mais convincente para justificar qualquer impacto potencial sobre as crianças. Seu RIPD é uma ferramenta útil para ajudá-lo a avaliar esse equilíbrio.

- **Função pública:** se você estiver oferecendo um serviço como parte de suas funções públicas ou executando uma tarefa específica de interesse público. Você precisa identificar uma base legal ou de direito comum para essa função ou tarefa.

É improvável que o consentimento seja a base mais apropriada para o tratamento que é necessário com o intuito de fornecer o serviço central. Isso porque o tratamento é uma condição do contrato, portanto, pedir um consentimento separado é desnecessário e potencialmente confuso. Ele corre o risco de diluir o conceito geral de consentimento como uma escolha clara e separada, sem compromisso, e pode contribuir para a 'fadiga de consentimento' (*consent fatigue*)[23]. Você só precisa do consentimento, quando especificamente exigido por outra disposição, como, por exemplo:

- para cumprir com as regras do RPCE – embora você não precise de consentimento para *cookies* que são estritamente necessários para seu serviço; ou
- para obter o consentimento explícito de elementos específicos de seu serviço que processam dados de categoria especial (mais sobre isso abaixo).

A obrigação legal pode ser relevante para alguma prevenção de fraude, proteção à criança ou medidas de salvaguarda, se você puder indicar uma disposição legal específica ou uma fonte apropriada de aconselhamento ou de orientação sobre suas obrigações legais.

É pouco provável que os interesses vitais sejam relevantes nesse contexto. Interesses legítimos são, provavelmente, uma base mais confiável para quaisquer medidas que você tome para proteger a saúde ou a segurança de uma criança.

Que base legal podemos usar para o tratamento 'não essencial'?

Por tratamento 'não essencial', entendemos o tratamento que não é parte integrante do fornecimento de seu serviço principal. Isso inclui tratamento para elementos opcionais do serviço ou tratamento para fins comerciais mais amplos, como marketing, melhoria do serviço ou modelos de financiamento indireto.

---

23. Termo original: *Consent fatigue*. Ver: <https://iapp.org/news/a/how-to-avoid-consent-fatigue/> ; <https://olhardigital.com.br/2021/01/20/noticias/google-diz-que-pedir-consentimento-do-usuario-para-tudo-seria-trabalhoso/>. Acesso em 25 de abril de 2021.

Você deve dar à criança (e seus pais, quando apropriado) a maior escolha possível sobre esses elementos de seu tratamento. Isso inclui, no mínimo, a implementação dos parâmetros deste código sobre configurações padrão de privacidade, minimização de dados, geolocalização e perfilamento.

Para elementos opcionais de seu serviço que uma criança tenha ativado especificamente, é preciso um contrato para qualquer tratamento que seja, objetivamente, necessário, a fim de entregar esse elemento específico do serviço, se a criança tiver capacidade para celebrar um contrato, da mesma forma que para o tratamento principal. Você também pode considerar os interesses legítimos. No entanto, para que esses sejam aplicáveis, você deve dar à criança escolhas separadas, no intuito de ativar cada elemento separado do serviço, sempre que isso for funcionalmente possível. Você não pode agrupar elementos independentes de um serviço. Veja também o padrão sobre a minimização de dados neste código.

Você não precisa do consentimento, de acordo com as regras de RPCE sobre *cookies*, desde que o tratamento seja estritamente necessário para esses elementos extras de um serviço e eles tenham sido solicitados pela criança. Há vantagens em usar interesses legítimos ou contrato, em vez de consentimento com base legal, para evitar pedidos repetidos de consentimento e a chamada 'fadiga de consentimento' (*consent fatigue*). Contudo, você ainda precisa estar em conformidade com os parâmetros deste código, relacionadas às configurações e aos controles de privacidade, mesmo que isso fique aquém de um mecanismo de consentimento completo.

Com o objetivo de consolidar a importância da escolha de uma criança, ou como uma salvaguarda contra um risco particular aos interesses de uma criança, você pode optar pelo consentimento, como base legal para um tratamento não essencial. Se o fizer, você precisa assegurar-se de utilizar um método de consentimento positivo que seja claro, separado de seus termos e condições, separado de suas informações de privacidade e fácil de retirar. Você também deve cumprir o Artigo 8, do RGPD (conforme adaptado pela seção 9, da DPA 2018), e obter o consentimento dos pais para crianças menores de 13 anos. Mais informações sobre esse assunto abaixo. Você também deve estar em conformidade com todos os parâmetros deste código, na medida em que eles sejam relevantes para seu serviço.

É importante lembrar que você precisa garantir, de acordo com o RPCE, o consentimento, conforme determinado pelo RGPD para quais-

quer *cookies*, aplicativos ou outras tecnologias relevantes que obtenham acesso ou armazenem dados no dispositivo do usuário, mas que não são estritamente necessários para o serviço. Você também deve observar a opinião do Conselho Europeu de Proteção de Dados (EDPB), sobre o tratamento para fins de publicidade comportamental on-line. A EDPB tem sido clara em considerar que interesses legítimos não serão uma base legal apropriada para o tratamento desse tipo de atividade on-line (o que deixa o consentimento como única base legal viável para o tratamento).

Se você estiver processando para fins comerciais mais amplos e não for pego pelas regras dos *cookies*, você ainda poderá considerar interesses legítimos, tarefa pública ou obrigação legal como possíveis bases legais, dependendo do porquê e como você está utilizando os dados.

Para informações além deste código:

Veja nossa seção de orientação sobre o assunto à parte:

- Consentimento
- Contrato
- Obrigação legal
- Função pública
- Interesses legítimos
- Guia ao RPCE - *Cookies* e tecnologias similares

Mais informações - Conselho Europeu de Proteção de Dados

O Conselho Europeu de Proteção de Dados (EDPB), que substituiu o Grupo de Trabalho do Artigo 29 (WP29), inclui representantes das autoridades de proteção de dados de cada Estado membro da UE. Ele adota diretrizes para o cumprimento das exigências do RGPD.

A EDPB publicou o 'Parecer 5/2019 sobre a interação entre a Diretiva e*Privacy* e o RGPD'. Esse documento fornece informações relevantes sobre como as regras de *cookies* se relacionam com o RGPD e reafirma as posições anteriormente tomadas pelo WP29, sobre quando o consentimento deve ser exigido para certas operações de tratamento, além da definição de *cookies*.

A WP29 publicou, anteriormente, o 'Parecer 3/2013 sobre a limitação da finalidade' e o 'Parecer 6/2014 sobre a noção de interesses legítimos'. Embora essas orientações tenham sido produzidas sob a estrutura anterior de proteção de dados, elas ainda se aplicam em grande parte, segundo o RGPD.

Quando temos que obter o consentimento dos pais?

O artigo 8(1), do RGPD (conforme modificado pela seção 9, da DPA 2018), estabelece que, se você estiver confiando no consentimento como sua base legal:

> "em relação à oferta direta de serviços da sociedade da informação às crianças, o tratamento de dados pessoais de uma criança será lícito, quando a criança tiver pelo menos [13] anos de idade. Quando a criança tiver menos de [13] anos de idade, o tratamento só é lícito se, e na medida em que, o consentimento for dado ou autorizado pelos titulares das responsabilidades parentais da criança.".

Isso não significa que você sempre tenha que obter o consentimento dos pais para usuários menores de 13 anos. Ele só se aplica se você disponibilizar seus serviços para crianças e se você confiar no consentimento como base legal (por exemplo, para qualquer tratamento não essencial, *cookies* ou tecnologias similares, ou tratamento de dados de categoria especial).

Se assim for, indica-se que você precisa fazer 'esforços razoáveis', a fim de obter e verificar o consentimento dos pais para crianças menores de 13 anos.

Você pode levar em conta a tecnologia disponível, ao decidir o que é razoável para os fins do Artigo 8. Você também pode considerar outras circunstâncias, incluindo seus recursos e o nível de risco identificado em seu RIPD, mas você deve ser capaz de justificar sua abordagem.

O cumprimento dos parâmetros deste código também deve ajudar. Isso porque os parâmetros deste código trabalham em conjunto para mitigar os riscos decorrentes do tratamento de dados pessoais das crianças. Se você estiver em conformidade com os parâmetros sobre aplicação adequada à idade (e aplicar os parâmetros a todos os usuários, quando não for possível estabelecer a idade com um nível de confiança adequado aos riscos), então você está fornecendo proteções significativas para crianças por padrão, mesmo que elas tenham mentido sobre sua idade. Isso significa que os riscos que podem surgir do desconhecimento da idade de um usuário, ou da não verificação do consentimento dos pais para um padrão elevado, são reduzidos. O consentimento dos pais torna-se apenas uma das várias medidas em vigor para proteger as crianças on-line.

Sua abordagem com relação à verificação da idade e ao consentimento dos pais, nos termos do Artigo 8 deve, portanto, ser compatível com sua abordagem em relação à aplicação adequada à idade, nos termos deste código.

Se você verificar a idade e a autoridade dos pais para fins do Artigo 8, então você precisa fazê-lo de uma forma compatível com a privacidade. Colete a quantidade mínima de 'identificadores difíceis' (como escaneamentos de passaportes ou detalhes de cartões de crédito). Lembre-se de que você precisa cumprir com o RGPD no tratamento de quaisquer dados pessoais coletados para fins de verificação, incluindo limitação da finalidade, minimização de dados, limitação de armazenamento e princípios de segurança.

Se você estiver usando um serviço de verificação de terceiros, você deve usar sistemas atribuídos, que oferecem uma resposta de sim/não, quando perguntado se um indivíduo está acima de uma determinada idade, ou se uma pessoa detém a responsabilidade parental sobre a criança.

Se você puder demonstrar que seu tratamento é, particularmente, de baixo impacto e não traz nenhum risco significativo para as crianças, você pode ser capaz de demonstrar que os mecanismos de autodeclaração são razoáveis por si mesmos (por exemplo, *cookies* analíticos).

Se os riscos forem maiores, então você precisa confiar em métodos mais robustos ou mitigar os riscos, aplicando os parâmetros deste código a todos os usuários, independentemente de sua idade autodeclarada.

Para informações além deste código:

Orientações detalhadas sobre o consentimento

Crianças e o RGPD - Quais são as regras sobre um SSI e consentimento?

E os dados sensíveis?

Se seu serviço on-line tratar quaisquer dados sensíveis de crianças, você deverá identificar, tanto uma base legal, relacionada ao Artigo 6, quanto uma condição adicional para o tratamento desses dados, sob o Artigo 9. Os dados de categoria especial incluem informações sobre:

- raça;
- origem étnica;
- política;
- religião;
- filiação a sindicatos;
- genética;
- identificação biométrica (por exemplo, reconhecimento / leitura facial ou de impressões digitais);

- saúde (incluindo dados coletados via aplicativos de *fitness* / exercícios);
- vida sexual; ou
- orientação sexual.

É provável que as condições mais relevantes do Artigo 9 sejam:

Artigo 9(2)(a) – consentimento explícito: Se você precisar tratar dados de categoria especial para fornecer um serviço ao indivíduo, pode haver consentimento explícito como condição para tratar esses dados, mesmo que seja uma condição de serviço. Porém, você deve estar confiante de que pode demonstrar que o consentimento ainda é dado livremente. Sobretudo, que o tratamento é objetivamente necessário para executar um elemento solicitado do serviço, e não agrupado com outros elementos do serviço ou incluído em seus termos para fins comerciais mais amplos.

Artigo 9(2)(d) - entidades sem fins lucrativos: se você se enquadra como uma entidade sem fins lucrativos e seu serviço on-line tem um objetivo político, filosófico, religioso ou sindical. A criança deve ser um membro ou alguém em contato regular com você para esses fins e você não deve revelar seus dados fora de sua organização sem consentimento. Você também deve cumprir todas as salvaguardas estabelecidas neste código, assim como outras salvaguardas apropriadas identificadas em seu RIPD.

Artigo 9(2)(g) - interesse público substancial: você pode se basear nesta condição se você puder atender a uma das 23 condições específicas de interesse público substancial estabelecidas no cronograma 1 da DPA 2018. Você também precisa de um 'documento de política apropriado' que estabeleça brevemente em que condição você está se baseando, como você cumpre com os princípios, bem como suas políticas de retenção e eliminação de dados (isso pode ser retirado do passo 4 de sua RIPD).

Talvez você possa considerar as condições específicas de interesse público substancial no cronograma 1, da DPA 2018, para:

- fins estatutários ou governamentais (condição 6);
- prevenção ou detecção de atos ilegais (condição 10);
- prevenção de fraudes (condição 14);
- ou proteção de crianças (condição 18).

Você deve revisar os detalhes dessas condições cuidadosamente. Se nenhuma outra condição específica estiver disponível, você deve obter o consentimento explícito válido da criança (ou de seus pais, se a criança for menor de 13 anos), caso contrário, você não poderá prosseguir com quaisquer tratamentos dos dados de categoria especial.

Você deve documentar e justificar sua condição como parte de seu RIPD.

Para informações além deste código:

Veja nossa orientação sobre dados sensíveis

Orientações detalhadas sobre consentimento

ANEXO D: MODELO DE RELATÓRIO DE IMPACTOS À PROTEÇÃO DE DADOS (RIPD)

Este código entrou em vigor em 2 de setembro de 2020, com doze meses de período de transição. Organizações devem se adequar até o dia 2 de setembro de 2021.

Este modelo é um exemplo de como você pode registrar seu processo e o resultado do RIPD para um serviço on-line provável de ser acessado por crianças. Ele é adaptado conforme nosso modelo geral de RIPD e segue o processo estabelecido em nossa orientação sobre RIPDs e no código de *design* adequado à idade. Deve ser lido junto com o código e a orientação sobre RIPDs, e com os Critérios para um RIPD aceitável, estabelecidos nas diretrizes europeias.

Você deve começar a preencher o modelo no início do *design* de seu serviço on-line ou no início de seu processo de desenvolvimento, se estiver fazendo uma mudança significativa em um serviço on-line existente que provavelmente será acessado por crianças. Os resultados devem ser integrados novamente no *design* de seu serviço.

SUBMETENDO OS DETALHES / INFORMAÇÕES DO CONTROLADOR
Nome do controlador:
Tema / Título do RIPD:
Nome do contato do controlador / DPO (deletar, se apropriado):

ETAPA 1: IDENTIFICAR A NECESSIDADE DE UM RIPD
Explique de forma detalhada a natureza de seu serviço on-line e o estágio atual de *design* ou desenvolvimento. Você pode achar útil consultar ou criar um link para outros documentos. Resumir quando e como você identificou a necessidade de um RIPD.

ETAPA 2: DESCREVER A NATUREZA DO TRATAMENTO DE DADOS

Descreva a natureza do tratamento: como você irá coletar, usar, armazenar e excluir dados? Quais são as fontes dos dados? Você vai compartilhar dados com alguém? Você pode achar útil consultar um diagrama de fluxo ou outra forma de descrever os fluxos de dados. Que tipos de tratamento identificados como de alto risco estão envolvidos? Seu serviço envolve algum perfilamento, alguma tomada de decisão automatizada ou algum elemento de geolocalização? Quais são seus planos (se houver) de assegurar ou controlar a idade? Quais são seus planos (se houver) para controles parentais?

Descrever o escopo do tratamento: qual é a natureza dos dados e se incluem dados sensíveis ou dados de infração criminal? Quantos dados serão coletados e utilizados? Com que frequência? Por quanto tempo você os guardará? Quantas pessoas são afetadas? Qual é a área geográfica coberta?

Descreva o contexto do tratamento: qual é a natureza do seu serviço? O *design* do seu serviço é adequado para crianças? Se não, é provável que crianças menores de 18 anos tenham acesso a ele de qualquer forma? Qual é a faixa etária provável de seus usuários? Qual o controle que eles terão? Eles entenderiam e esperariam que você usasse seus dados desta maneira? Seu serviço utiliza alguma técnica de encorajamento? Há preocupações prévias sobre serviços similares ou falhas de segurança particulares? Seu serviço é novo de alguma forma? Qual é o estado atual da tecnologia nesta área? Há alguma questão atual de preocupação pública que você deva considerar, particularmente sobre os riscos on-line para crianças? Existem normas relevantes do setor, códigos de prática ou orientação pública nessa área? Que responsabilidades você tem sob a legislação de igualdade aplicável para a Escócia, o País de Gales e a Irlanda do Norte? Existe alguma orientação ou pesquisa relevante sobre as necessidades de desenvolvimento, bem-estar ou capacidade das crianças na faixa etária relevante? Você assinou algum código de conduta ou esquema de certificação aprovado (uma vez que algum tenha sido aprovado)?

Descreva as finalidades do tratamento: o que você quer alcançar com seu serviço? Qual é o efeito pretendido sobre as pessoas? Quais são os benefícios do tratamento – para você, e de forma mais ampla? Quais são os benefícios específicos pretendidos para as crianças?

ETAPA 3: PROCESSO DE CONSULTA

Considerar como consultar as partes interessadas relevantes: descrever quando e como você buscará a opinião dos indivíduos – e, especificamente, como você buscará a opinião das crianças e dos pais – ou justificar por que não é possível fazer isso. Quem mais você precisa envolver dentro de sua organização? Você precisa pedir a ajuda de seus operadores? Você planeja consultar especialistas em direitos das crianças e necessidades de desenvolvimento? Se não, por que não? Você planeja consultar algum outro especialista?

ETAPA 4: AVALIAR A NECESSIDADE E A PROPORCIONALIDADE

Descreva as medidas de conformidade e proporcionalidade, sobretudo: qual é sua base legal para o tratamento? O tratamento atinge seu objetivo? Existe outra maneira de alcançar o mesmo resultado? Como você evitará o desvirtuamento da função? Como você vai garantir a qualidade e a minimização dos dados? Se você usa uma IA, como evitará o vício e explicará seu uso? Que informações você dará aos indivíduos? Como você ajudará a apoiar seus direitos? Que medidas você tomará para garantir que os operadores cumpram? Como você protege qualquer transferência internacional?

Descreva como você está em conformidade com o Código de *Design* Apropriado para a Idade: que medidas específicas você tomou para cumprir com cada um dos parâmetros do código?

1. O melhor interesse da criança:
2. Relatório de Impacto à Proteção de Dados (RIPD):
3. Aplicação adequada à idade:
4. Transparência:
5. Uso indevido de dados:
6. Políticas e padrões da comunidade:
7. Configurações padrão:
8. Minimização de dados:
9. Compartilhamento de dados:
10. Geolocalização:
11. Controles parentais:
12. Perfilamento:
13. Técnicas de *Nudge*:
14. Brinquedos e dispositivos conectados:
15. Ferramentas On-line:

ETAPA 5: IDENTIFICAR E AVALIAR OS RISCOS			
Descrever fontes de riscos e natureza do impacto potencial sobre os indivíduos. Incluir, no mínimo, uma avaliação de riscos específicos para crianças, conforme listado no padrão RIPD, no código de *design* apropriado para a idade. Talvez seja necessário considerar separadamente para diferentes faixas etárias.	**Probabilidade de dano**	**Severidade do dano**	**Risco geral**
	Remota, possível, ou provável	Mínima, significativa ou severa	Baixo, médio ou alto
Descrever fontes de riscos e natureza do impacto potencial sobre os indivíduos. Incluir, no mínimo, uma avaliação de riscos específicos para crianças, conforme listado no padrão sobre RIPDs, no código de *design* apropriado para a idade. Talvez seja necessário considerar separadamente para diferentes faixas etárias.	**Probabilidade de dano**	**Severidade do dano**	**Risco geral**

ETAPA 6: IDENTIFICAR MEDIDAS PARA DIMINUIR OS RISCOS			
Identificar medidas adicionais que você poderia tomar para reduzir ou eliminar riscos identificados como de médio ou alto risco na etapa 5.			
Risco	**Opções para reduzir ou eliminar o risco**	**Efeito no risco**	**Risco residual**
		Eliminado Reduzido Aceito	Baixo Médio Alto

ETAPA 7: ASSINAR E REGISTRAR OS RESULTADOS		
Item	**Nome/ Cargo / Data**	**Anotações**
Medidas aprovadas por:		Integrar ações de volta ao plano do projeto, com data e responsabilidade pela conclusão
Riscos residuais aprovados por:		Se aceitar qualquer risco elevado residual, consulte a ICO antes de prosseguir
Parecer / conselhos do DPO por:		O DPO deve aconselhar sobre a conformidade, as medidas da etapa 6 e se o tratamento pode prosseguir
Resumo do parecer / conselhos do DPO:		
Parecer / conselhos do DPO aceito ou anulado por:		Se rejeitado, você deve se justificar
Comentários:		
Respostas de consulta revisadas por:		Se sua decisão se afastar do ponto de vista individual, você deve esclarecer suas motivações
Comentários:		
Esse RIPD ficará sob a revisão por:		O DPO também deve analisar a conformidade contínua com o RIPD

AGRADECIMENTOS

Essa tradução contou com a generosa contribuição da pesquisadora **Janaina Costa** e dos pesquisadores **Christian Perrone**, **João Francisco de Aguiar Coelho** e **Matheus Mantuani**.

Esse relatório contou com o generoso
apoio financeiro do Governo do Reino Unido
através do Programa de Acesso Digital

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org