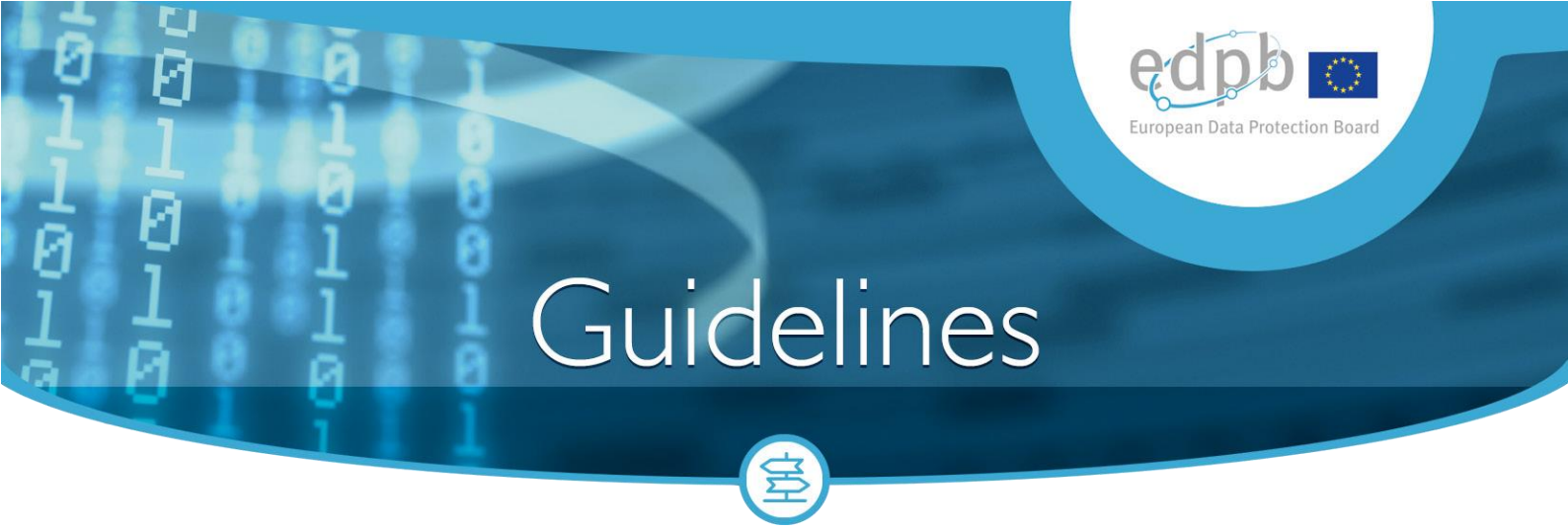


Diretrizes 03/2022 sobre

Padrões de design enganosos em interfaces de plataformas de mídia social:

como reconhecê-los e evitá-los

Versão 2.0

Adotado em 14 de fevereiro de 2023

Histórico das versões

Versão 2.0	14 de fevereiro de 2023	Adoção das Diretrizes após consulta pública
Versão 1.0	14 de março de 2022	Adoção das Diretrizes para consulta pública

RESUMO EXECUTIVO

Estas Diretrizes oferecem recomendações práticas aos provedores de mídia social como controladores de mídia social, designers e usuários de plataformas de mídia social sobre como avaliar e evitar os chamados "padrões de design enganosos" nas interfaces de mídia social que infringem as exigências da GDPR. Para este fim, a EDPB recomenda que os controladores façam uso de equipes interdisciplinares, compostas, entre outros, por designers, responsáveis pela proteção de dados e tomadores de decisão. É importante observar que a lista de padrões de design enganosos e melhores práticas, bem como os casos de uso, não são exaustivos. Os provedores de mídia social permanecem responsáveis e responsáveis por garantir a conformidade da GDPR de suas plataformas.

Padrões de design enganoso em interfaces de plataformas de mídia social

No contexto destas Diretrizes, "padrões de design enganosos" são considerados como interfaces e viagens de usuários implementadas em plataformas de mídia social que tentam influenciar os usuários a tomar decisões não intencionais, não intencionais e potencialmente prejudiciais, muitas vezes em direção a uma decisão que é contra os melhores interesses dos usuários e a favor dos interesses das plataformas de mídia social, no que diz respeito ao processamento de seus dados pessoais. Os padrões de design enganosos visam influenciar o comportamento dos usuários e podem dificultar sua capacidade de proteger efetivamente seus dados pessoais e fazer escolhas conscientes. As autoridades de proteção de dados são responsáveis por sancionar o uso de padrões de design enganosos se estes violarem os requisitos da GDPR. Os padrões de design enganosos abordados dentro destas Diretrizes podem ser divididos nas seguintes categorias:

- ***A sobrecarga*** significa que os usuários são confrontados com uma avalanche/grande quantidade de solicitações, informações, opções ou possibilidades, a fim de estimulá-los a compartilhar mais dados ou permitir, involuntariamente, o processamento de dados pessoais contra as expectativas da pessoa em questão. Os três seguintes tipos de padrões de projeto enganosos se enquadram nesta categoria: ***Incitação contínua***, ***Labirinto de Privacidade*** e ***Demasiadas Opções***

- ***Pular*** significa projetar a interface ou a viagem do usuário de uma forma que os usuários esqueçam ou não pensem em todos ou alguns dos aspectos da proteção de dados.
  Os dois seguintes tipos de padrões de design enganosos se enquadram nesta categoria:
  Aconchego enganoso
  e ***olhe para lá***

- ***A agitação*** afeta a escolha que os usuários fariam ao apelar para suas emoções ou ao usar empurrões visuais.
  Os dois seguintes tipos de padrões de design enganosos se enquadram nesta categoria: ***Direção Emocional***
  e ***Escondido à vista de todos***

- ***Obstruir*** significa dificultar ou bloquear os usuários em seu processo de se informar ou gerenciar seus dados, tornando a ação difícil ou impossível de ser realizada.

Os três seguintes tipos de padrões de design enganosos se enquadram nesta categoria: ***Beco sem saída***, ***mais longo do que o necessário*** e ***ação enganosa***

- ***Fickle*** significa que o design da interface é inconsistente e não claro, tornando difícil para o usuário navegar pelas diferentes ferramentas de controle de proteção de dados e entender a finalidade do processamento.
  Os seguintes quatro tipos de padrões de design enganosos se enquadram nesta categoria: ***Hierarquia ausente, Descontextualização, Interface Inconsistente*** e ***Descontinuidade de Linguagem***

- ***Deixado no escuro*** significa que uma interface é projetada de forma a ocultar informações ou ferramentas de controle de proteção de dados ou para deixar os usuários inseguros sobre como seus dados são processados e que tipo de controle eles podem ter sobre o exercício de seus direitos.
  Os dois seguintes tipos de padrões de design enganosos se enquadram nesta categoria: ***Informações contraditórias*** e ***palavras ou informações ambíguas***

Disposições relevantes do GDPR para avaliações enganosas de padrões de projeto

Quanto à conformidade da proteção de dados das interfaces de usuário de aplicações on-line dentro do setor de mídia social, os princípios de proteção de dados aplicáveis são estabelecidos no artigo 5 GDPR. O princípio do processamento justo estabelecido no Artigo 5 (1) (a) GDPR serve como ponto de partida para avaliar se um padrão de desenho realmente constitui um "padrão de desenho enganoso". Outros princípios que desempenham um papel nesta avaliação são os de transparência, minimização de dados e responsabilidade nos termos do Artigo 5 (1) (a),
(c) e (2) GDPR, bem como, em alguns casos, a limitação de propósito sob o Artigo 5 (1) (b) GDPR. Em outros casos, a avaliação legal também se baseia nas condições de consentimento sob os Artigos 4 (11) e 7 GDPR ou outras obrigações específicas, tais como o Artigo 12 GDPR. Evidentemente, no contexto dos direitos do sujeito dos dados, o terceiro capítulo da GDPR também precisa ser levado em consideração. Finalmente, os requisitos de proteção de dados por desenho e default sob o Artigo 25 GDPR desempenham um papel vital, pois aplicá-los antes de lançar um desenho de interface ajudaria os provedores de mídia social a evitar padrões de desenho enganosos em primeiro lugar.

Exemplos de padrões de design enganosos em casos de uso do ciclo de vida de uma conta de mídia social

As disposições da GDPR se aplicam a todo o curso do processamento de dados pessoais como parte da operação de plataformas de mídia social, ou seja, a todo o ciclo de vida de uma conta de usuário. A EDPB dá exemplos concretos de padrões de design enganosos para os seguintes diferentes casos de uso dentro deste ciclo de vida: a inscrição, ou seja, o processo de registro; os casos de uso de informações relativas à notificação de privacidade, controle conjunto e comunicações de violação de dados; gerenciamento de consentimento e proteção de dados; exercício dos direitos do sujeito dos dados durante o uso das mídias sociais; e, finalmente, o fechamento de uma conta de mídia social. As conexões com as disposições da GDPR são explicadas de duas maneiras: primeiro, cada caso de uso explica com mais detalhes quais das disposições da GDPR acima mencionadas são particularmente relevantes para ela. Em segundo lugar, os parágrafos que envolvem os exemplos de padrões de design enganosos explicam como estes infringem a GDPR.

Recomendações de melhores práticas

Além dos exemplos de padrões de design enganosos, as Diretrizes também apresentam as melhores práticas no final de cada caso de uso, bem como no Anexo II destas Diretrizes. Estas contêm recomendações específicas para a concepção de interfaces de usuário que facilitam a implementação efetiva do GDPR.

Lista de verificação de categorias de padrões de design enganosos

Uma lista de verificação de categorias de padrões de design enganosos pode ser encontrada no Anexo I a estas Diretrizes. Ela fornece uma visão geral das categorias acima mencionadas e dos tipos de padrões de design enganosos, juntamente com uma lista dos exemplos para cada padrão que são mencionados nos casos de uso. Alguns leitores podem achar útil usar a lista de verificação como um ponto de partida para descobrir estas Diretrizes.

Tabela de conteúdo

O Conselho Europeu de Proteção de Dados

Tendo em conta o artigo 70 e (1e) do Regulamento 2016/679/UE do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE, (doravante "GDPR"),

Tendo em conta o Acordo EEE e, em particular, o Anexo XI e o Protocolo 37, emendado pela Decisão do Comitê Misto do EEE nº 154/2018 de 6 de julho de 2018,[1]

Tendo em conta o Artigo 12 e o Artigo 22 de seu Regulamento Interno,

ADOTOU AS SEGUINTES DIRETRIZES

1 ESCOPO

1. O objetivo destas Diretrizes é fornecer recomendações e orientações para o projeto das interfaces das plataformas de mídia social. Para os objetivos destas Diretrizes, as mídias sociais são entendidas como plataformas on-line que permitem o desenvolvimento de redes e comunidades de usuários, entre as quais informações e conteúdo são compartilhados.[2] As Diretrizes podem ser usadas tanto na fase de concepção de uma interface de usuário, para evitar a implementação de padrões de design enganosos.[3] desde o início, ou em um serviço existente, para avaliar a conformidade de sua interface. Eles são destinados a provedores de mídia social como controladores de mídia social, que têm a responsabilidade pelo projeto e operação de plataformas de mídia social. A este respeito, as Diretrizes visam lembrar as obrigações provenientes da GDPR, com especial referência aos princípios de legalidade, justiça, transparência, limitação de propósito e minimização de dados no projeto de interfaces de usuário e apresentação de conteúdo de seus serviços e aplicativos web. Os princípios acima mencionados devem ser implementados de forma substancial e, de uma perspectiva técnica, constituem requisitos para o projeto de software e serviços, incluindo interfaces de usuário. É feito um estudo aprofundado sobre os requisitos da GDPR quando aplicados às interfaces de usuário e apresentação de conteúdo, e será esclarecido o que deve ser considerado um "padrão de design enganoso", uma forma de projetar e apresentar conteúdo que viole substancialmente esses requisitos, enquanto ainda finge cumprir formalmente. Estas Diretrizes também são adequadas para aumentar a conscientização dos usuários sobre seus direitos, e os riscos possivelmente advindos do compartilhamento de muitos dados ou do compartilhamento de seus dados de forma descontrolada. Estas Diretrizes também visam educar os usuários a reconhecer "padrões de design enganosos" (conforme definido a seguir), e como enfrentá-los para proteger sua privacidade de forma consciente. Como parte da análise, o ciclo de vida de uma conta de mídia social foi examinado com base em cinco casos de uso: "Abrir uma conta de mídia social" (caso de uso 1), "Manter-se informado sobre a mídia social" (caso de uso 2), "Manter-se protegido sobre a mídia social" (caso de uso 3), "Manter-se direito sobre a mídia social":

[1] As referências a "Estados-membros" feitas ao longo deste documento devem ser entendidas como referências a "Estados membros da AEA".

[2] Definição idêntica às Diretrizes 08/2020 da EDPB sobre o direcionamento de usuários de mídias sociais, para.

1, ver nota de rodapé 1 para descrição mais detalhada; disponível em https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

[3] Para a versão 2.0 destas Diretrizes, a EDPB está usando o termo mais inclusivo e descritivo "padrão de design enganoso" em vez de "padrão escuro".

direitos do interessado" (caso de uso 4) e "Adeus e longevidade: deixar uma conta na mídia social" (caso de uso 5).

2. Nestas Diretrizes, o termo "interface do usuário" corresponde aos meios para que as pessoas interajam com as plataformas de mídia social. O documento focaliza as interfaces gráficas de usuário (por exemplo, usadas para interfaces de computador e smartphone), mas algumas das observações feitas podem também se aplicar a interfaces controladas por voz (por exemplo, usadas para falantes inteligentes) ou interfaces baseadas em gestos (por exemplo, usadas em realidade virtual). O termo "viagem do usuário" corresponde à série de ações ou passos a serem executados pelos usuários para atingir seu objetivo que, nas redes sociais, podem ser coisas como navegar em seu feed, compartilhar um post, definir suas preferências, etc. O termo "experiência do usuário" corresponde à experiência geral que os usuários têm com as plataformas de mídia social, que inclui a utilidade percebida, a facilidade de uso e a eficiência de interagir com ela. O design da interface do usuário e o design da experiência do usuário têm evoluído continuamente durante a última década. Mais recentemente, eles se conformaram com a ubiqüidade, personalização e as chamadas interações e experiências de usuário sem interrupção: a interface perfeita deve ser altamente personalizada, fácil de usar e multimodal.[4] Embora essas tendências possam aumentar a facilidade de uso dos serviços digitais, elas podem ser usadas de tal forma que promovam principalmente comportamentos de usuário que vão contra o espírito do GDPR.[5] Isto é especialmente relevante no contexto da economia da atenção, onde a atenção do usuário é considerada uma mercadoria. Nesses casos, os limites legalmente permitidos da GDPR podem ser excedidos e o design da interface e o design da experiência do usuário que leva a tais casos são descritos abaixo como "padrões de design enganosos".

3. No contexto destas Diretrizes, "padrões de design enganosos" são considerados interfaces e viagens de usuários implementadas em plataformas de mídia social que visam influenciar os usuários a tomar decisões não intencionais, respectivamente de má vontade e/ou potencialmente prejudiciais, muitas vezes em direção a uma opção que é contra os melhores interesses dos usuários e a favor dos interesses das plataformas de mídia social, no que diz respeito aos seus dados pessoais. Os padrões de design enganosos visam influenciar o comportamento dos usuários, geralmente confiando em preconceitos cognitivos, e podem prejudicar sua capacidade de "proteger efetivamente seus dados pessoais e fazer escolhas conscientes".[6]Por exemplo, tornando-os incapazes de "dar um consentimento livre e esclarecido".[7] Isto pode ser explorado em vários aspectos do projeto, tais como as escolhas de cores das interfaces e a colocação do conteúdo. Por outro lado, fornecendo incentivos e desenhos de fácil utilização, a realização de regulamentos de proteção de dados pode ser apoiada.

4. Padrões de projeto enganosos não levam necessariamente apenas a uma violação das normas de proteção de dados. Padrões de design enganosos também podem, por exemplo, violar os regulamentos de proteção ao consumidor. Os limites entre as infrações aplicáveis pelas autoridades de proteção de dados e aquelas aplicáveis pelas autoridades nacionais de proteção ao consumidor, concorrência ou outras autoridades, podem se sobrepor.[8] De acordo com a GDPR,

[4] Para mais detalhes ver CNIL, Relatório IP No. 6: Shaping Choices in the Digital World, 2019. p. 9 https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[5] CNIL, Shaping Choices in the Digital World, 2019. p. 10.

[6] CNIL, Shaping Choices in the Digital World, 2019. p. 27.

[7] Ver Conselho Norueguês do Consumidor, *Enganado pelo design: Como as empresas de tecnologia usam padrões escuros para nos desencorajar de exercer nossos direitos de privacidade*, p. 10

https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-_27-decididos_por_projeto-final.pdf, mas também CNIL, Shaping Choices in the Digital World, p. 30, 31.

[8] A este respeito, o Artigo 25 (2) do Regulamento (UE) 2022/2065 de 19 de outubro de 2022 sobre um mercado único para serviços digitais e que altera a Diretiva 2000/31/CE (Lei de Serviços Digitais), esclarece que a proibição de enganar ou manipular desenhos de interfaces on-line nos termos de seu Artigo 25 (1) não se aplicará às práticas cobertas pela Diretiva 2005/29/CE (Diretiva relativa às práticas comerciais desleais entre empresas e consumidores, UCPD) ou pela

As autoridades de proteção de dados são responsáveis por sancionar o uso de padrões de projeto enganosos se realmente violarem as normas de proteção de dados e, portanto, a GDPR. As violações das exigências da GDPR precisam ser avaliadas caso a caso. Somente padrões de design enganosos que possam se enquadrar neste mandato regulatório são cobertos por estas Diretrizes. Por esta razão, além de exemplos de padrões de design enganosos, as Diretrizes também apresentam melhores práticas que podem ser usadas para projetar interfaces de usuário que facilitem a implementação efetiva da GDPR. Tais melhores práticas podem oferecer um primeiro passo para uma maneira padronizada de os usuários controlarem efetivamente seus dados e exercerem seus direitos.

5. Os padrões de design enganosos[9] abordados dentro destas Diretrizes resultam de uma análise interdisciplinar das interfaces existentes e podem ser divididos nas seguintes categorias:

   Sobrecarga: os usuários são confrontados com uma avalanche/grande quantidade de solicitações, informações, opções ou possibilidades, a fim de estimulá-los a compartilhar mais dados ou permitir, involuntariamente, o processamento de dados pessoais contra as expectativas do sujeito dos dados.

   Pular: projetar a interface ou a viagem do usuário de uma forma que os usuários esqueçam ou não pensem em todos ou alguns dos aspectos da proteção de dados.

   Agitação: afeta a escolha que os usuários fariam ao apelar para suas emoções ou ao usar empurrões visuais.

   Obstrução: uma obstrução ou bloqueio dos usuários em seu processo de se informar ou gerenciar seus dados, tornando a ação difícil ou impossível de ser realizada.

   Fickle: o design da interface é inconsistente e não claro, tornando difícil para os usuários navegar pelas diferentes ferramentas de controle de proteção de dados e entender a finalidade do processamento.

   Deixado no escuro: uma interface é projetada de forma a ocultar informações ou ferramentas de controle de proteção de dados ou para deixar os usuários inseguros sobre como seus dados são processados e que tipo de controle eles podem ter sobre o exercício de seus direitos.

6. Além de reagrupar padrões de design enganosos nestas categorias de acordo com seus efeitos no comportamento dos usuários, estes padrões também podem ser divididos em padrões baseados em conteúdo e baseados em interface para tratar mais especificamente de aspectos da interface do usuário ou da jornada do usuário. Os padrões baseados no conteúdo referem-se ao conteúdo real e, portanto, também à redação e ao contexto das frases e dos componentes de informação. Além disso, porém, há também componentes que têm uma influência direta na percepção desses fatores. Estes padrões baseados em interface estão relacionados com as formas de exibição do conteúdo, navegação através dele ou interação com ele.

7. É essencial ter em mente que padrões de design enganosos levantam preocupações adicionais com relação ao impacto potencial sobre as crianças,[10] registrando-se na plataforma de mídia social, e também outros grupos vulneráveis de pessoas como idosos, pessoas com deficiência visual, ou não tão alfabetizados digitalmente como os outros. Grupos vulneráveis, tais como usuários idosos, são freqüentemente não apenas menos capazes de identificar práticas de projeto manipuladoras, mas também menos conscientes de que seu comportamento digital está sujeito a influência. A GDPR exige salvaguardas adicionais quando o processamento é sobre dados pessoais de crianças, pois estas últimas podem estar menos conscientes dos riscos e conseqüências relacionadas aos seus direitos ao processamento.[11]

PIBR. Além disso, a Nota da Comissão da UE (2021/C 526/01) oferece orientação sobre a interpretação e aplicação da UCPD, inclusive sobre "padrões escuros" em sua Seção 4.2.7.

[9] As categorias de padrões de design enganosos e tipos de padrões de design enganosos dentro dessas categorias serão exibidos em ***negrito e itálico*** no texto das Diretrizes. Uma visão detalhada é fornecida no Anexo.

[10] Ver também o considerando 81, frase 4, do Regulamento (UE) 2022/2065 (Lei de Serviços Digitais).

[11] GDPR, considerando 38.

O considerando 58 afirma explicitamente que quando o processamento for dirigido a uma criança, qualquer informação deve ser dada em uma linguagem clara e clara que as crianças possam facilmente entender. Além disso, a GDPR inclui explicitamente o processamento de dados de indivíduos, particularmente de crianças, para estar entre as situações em que o risco para os direitos e liberdades dos indivíduos de probabilidade e severidade variáveis, pode resultar do processamento de dados que poderia levar a danos físicos, materiais ou não materiais.[12]

8. Tendo em mente o acima exposto, deve ser entendido que os padrões de design enganosos não são exclusivos das plataformas de mídia social. Fortes opiniões sobre esta questão foram expressas durante a consulta pública destas Diretrizes. As interfaces estão presentes em muitos outros casos onde os usuários interagem com produtos e serviços baseados ou relacionados com operações de processamento de dados. Estes podem incluir websites e banners de cookies,[13] lojas on-line, videogames, aplicativos móveis e micropagamentos, etc. Embora os padrões de design enganosos descritos abaixo possam não estar presentes exatamente na mesma forma, suas variações ainda podem infringir os direitos dos sujeitos dos dados ou dos consumidores. No entanto, estas Diretrizes se concentram exclusivamente em padrões de design enganosos em plataformas de mídia social, já que a influência destas plataformas na vida diária das pessoas e nações está em constante crescimento, o que foi deixado claro em documentos anteriores da EDPB.[14]

2 PRINCÍPIOS APLICÁVEIS - O QUE TER EM MENTE?

9. Quanto à conformidade da proteção de dados das interfaces de usuário de aplicações on-line dentro do setor de mídia social, os princípios de proteção de dados aplicáveis são estabelecidos no artigo 5 GDPR. O princípio do processamento justo estabelecido no artigo 5 (1) (a) GDPR é um ponto de partida para uma avaliação da existência de padrões de design enganosos. Como a EDPB já declarou, a equidade é um princípio geral que exige que os dados pessoais não sejam processados de forma prejudicial, discriminatória, inesperada ou enganosa para a pessoa em questão.[15] Se a interface tiver informações insuficientes ou enganosas para os usuários e preencher as características de padrões de design enganosos, ela pode ser classificada como processamento injusto. O princípio da imparcialidade tem uma função guarda-chuva e todos os padrões de design enganosos não o cumpririam, independentemente do cumprimento de outros princípios de proteção de dados.

10. Além desta disposição fundamental de justiça no processamento, os princípios de responsabilidade, transparência e a obrigação de proteção de dados por projeto, estabelecidos no artigo 25 GDPR, também são relevantes no que diz respeito à estrutura de projeto e padrões de projeto enganosos podem infringir essas disposições. Entretanto, também é possível que a avaliação legal de padrões de design enganosos possa ser baseada nos elementos

[12] GDPR, considerando 75; ver também as Diretrizes 8/2020 da EDPB sobre o direcionamento dos usuários das mídias sociais, para. 16 https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

[13] Causado por uma série de reclamações recebidas da NOYB, uma força-tarefa da EDPB trocou opiniões sobre uma série de elementos de design em banners de cookies. O denominador comum acordado pelas AS em sua interpretação do quadro legal aplicável em várias camadas foi resumido em um "Relatório do trabalho realizado pela Força Tarefa de Banners de Biscoitos" de 17 de janeiro de 2023, disponível em https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_pt.pdf.

[14] Diretrizes 8/2020 da EDPB sobre o direcionamento dos usuários das mídias sociais, Declaração 2/2019 sobre o uso de dados pessoais no curso de campanhas políticas https://edpb.europa.eu/our-work-

tools/our- documentos/declarações/declarações-22019-use-pessoal-data-curso-político_pt.

[15] Diretrizes 4/20219 da EDPB sobre Proteção de Dados por Projeto e por Default, versão 2.0, adotadas em 20 de outubro de 2020, p. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019- article-25-data-protection-design-and_en.

sobre definições gerais tais como o Artigo 4 (11) GDPR, a definição de consentimento ou outras obrigações específicas tais como o Artigo 12 GDPR. O Artigo 12 (1) frase 1 da GDPR exige que os controladores tomem as medidas apropriadas para fornecer qualquer comunicação relacionada aos direitos do sujeito dos dados, bem como qualquer informação, de forma concisa, transparente, inteligível e facilmente acessível, usando linguagem clara e clara. Como mostra a frase 3 do considerando 39 sobre o princípio da transparência, esta exigência não se limita, entretanto, aos avisos de proteção de dados[16] ou direitos do sujeito dos dados,[17] mas se aplica a qualquer informação e comunicação relacionada ao processamento de dados pessoais. A frase 5 do considerando também esclarece que as pessoas em questão devem ser conscientizadas dos riscos, regras, salvaguardas e direitos em relação ao processamento de dados pessoais e como exercer seus direitos em relação a tal processamento.

11. Para a concepção de interfaces de usuário de aplicações on-line, também é importante levar em conta o princípio da limitação da finalidade sob o Artigo 5 (1) (b) GDPR, bem como o princípio da minimização de dados sob o Artigo 5 (1) (c) GDPR. Em qualquer caso, para garantir o cumprimento da proteção de dados, os controladores são bem aconselhados a verificar novamente o cumprimento de todos os princípios de proteção de dados de acordo com a GDPR.

2.1 Prestação de contas

12. O princípio de responsabilidade tem que ser refletido em cada projeto de interface de usuário.

13. Artigo 5 (2) A GDPR estabelece que um controlador será responsável e poderá demonstrar o cumprimento dos princípios da GDPR descritos no artigo 5 (1) da GDPR. Portanto, este princípio está intimamente ligado aos princípios relevantes mencionados acima. A prestação de contas pode ser fornecida por elementos que comprovem a conformidade do fornecedor da mídia social com a GDPR. A interface do usuário e a jornada do usuário podem ser usadas como uma ferramenta de documentação para demonstrar que os usuários, durante suas ações na plataforma de mídia social, leram e levaram em conta informações sobre proteção de dados, deram livremente seu consentimento, exerceram facilmente seus direitos, etc. Métodos qualitativos e quantitativos de pesquisa de usuários, tais como testes A/B, rastreamento visual ou entrevistas com usuários, seus resultados e suas análises também podem ser usados para apoiar a demonstração de conformidade. É importante observar que tais métodos de pesquisa muitas vezes também envolvem o processamento de dados pessoais, o que, portanto, precisa estar de acordo com a GDPR. Se, por exemplo, os usuários tiverem que marcar uma caixa ou clicar em uma das várias opções de proteção de dados, as telas das interfaces podem servir para mostrar o caminho dos usuários através das informações de proteção de dados e explicar como os usuários estão tomando uma decisão informada. Os resultados das pesquisas de usuários feitas nesta interface trariam elementos adicionais detalhando porque a interface é ótima para atingir um objetivo de informação.

14. Na área de interfaces de usuário, tais elementos documentais podem ser encontrados na divulgação de certos acordos e, acima de tudo, quando são obtidas provas, por exemplo, de dar consentimento ou uma confirmação de leitura.

2.2 Transparência

15. O princípio da transparência no Artigo 5 (1) (a) GDPR tem uma grande sobreposição com a área de responsabilidade geral. Mesmo que os controladores tenham que proteger certas informações comerciais sensíveis para terceiros, tornar a documentação sobre o processamento acessível ou gravável poderia ajudar a prestar contas: A confirmação da leitura pode ser obtida, por exemplo, para um texto que o controlador deve disponibilizar de acordo com o princípio de transparência. Isto pode sempre servir, ao mesmo tempo, para garantir a transparência em relação às pessoas em

questão.

[16] Abordado na parte 3.2. - use o caso 2a destas Diretrizes.
[17] Abordados nos casos de uso 4 e 5, ou seja, as partes 3.4 e 3.5 destas Diretrizes.

16. Todos os princípios de proteção de dados estabelecidos no artigo 5 GDPR são especificados com mais detalhes no GDPR. O artigo 5 (1) (a) GDPR estipula que os dados pessoais devem ser processados de forma transparente em relação à pessoa em questão. As Diretrizes sobre Transparência especificam os elementos de transparência estabelecidos pelo Artigo 12 GDPR, ou seja, a necessidade de fornecer as informações de forma "concisa, transparente, inteligível e facilmente acessível, usando linguagem clara e clara".[18] Estas Diretrizes também fornecem orientações sobre como cumprir as obrigações de informação previstas nos artigos 13 e 14 da GDPR em relação aos provedores de mídia social.

17. Além disso, o texto dos princípios de proteção de dados do Artigo 5 (1) (a) GDPR e outras disposições legais especiais dentro do Regulamento contêm muitos mais detalhes do princípio de transparência, que estão ligados a princípios legais específicos, tais como os requisitos especiais de transparência do Artigo 7 GDPR para obtenção de consentimento.

2.3 Proteção de dados por projeto e padrão

18. O artigo 25 (1) da GDPR especifica que os controladores devem implementar medidas técnicas e organizacionais adequadas, que são concebidas para implementar os princípios de proteção de dados, enquanto o artigo 25 (2) da GDPR esclarece que tais medidas também devem ser implementadas para garantir que, por padrão, somente os dados pessoais necessários para cada finalidade específica de processamento sejam processados. No contexto das Diretrizes 04/2019 sobre Proteção de Dados por Projeto e por Padrão do Artigo 25, há alguns elementos-chave que os controladores e processadores têm que levar em consideração ao implementar a proteção de dados por projeto em relação a uma plataforma de mídia social. Um deles é que, com relação ao princípio da justiça, as informações e opções de processamento de dados devem ser fornecidas de forma objetiva e neutra, evitando qualquer linguagem ou projeto enganoso ou manipulador.[19] As Diretrizes identificam elementos dos princípios de proteção de dados por padrão e proteção de dados por projeto, entre outras coisas, que se tornam ainda mais relevantes no que diz respeito a padrões de projeto enganosos:[20]

- Autonomia - Os sujeitos dos dados devem ter o maior grau de autonomia possível para determinar o uso feito de seus dados pessoais, bem como autonomia sobre o escopo e as condições desse uso ou processamento.
- Interação - Os titulares dos dados devem ser capazes de comunicar e exercer seus direitos em relação aos dados pessoais processados pelo controlador.
- Expectativa - O processamento deve corresponder às expectativas razoáveis dos sujeitos dos dados.
- Escolha do consumidor - Os controladores não devem "travar" seus usuários de maneira injusta. Sempre que um serviço de processamento de dados pessoais for proprietário, ele poderá criar um bloqueio ao serviço, o que pode não ser justo, se prejudicar a possibilidade das pessoas em questão de exercer seu direito de portabilidade de dados, de acordo com o Artigo 20 GDPR.
- Equilíbrio de poder - O equilíbrio de poder deve ser um objetivo chave da relação entre o controlador e o assunto. Os desequilíbrios de poder devem ser evitados. Quando isso não for possível, eles devem ser reconhecidos e contabilizados com contramedidas adequadas.
- Nenhuma decepção - Informações e opções de processamento de dados devem ser fornecidas de forma objetiva e neutra, evitando qualquer linguagem ou projeto enganoso ou manipulador.

[18] Artigo 29 Diretrizes do Grupo de Trabalho sobre transparência nos termos do Regulamento 2016/679, endossado pela EDPB https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[19] Ver Diretrizes 04/20219 sobre Proteção de Dados por Projeto e por Default, p. 18, para. 70.
[20] Trecho - para a lista completa, ver Diretrizes sobre Proteção de Dados por Projeto e por Default, para. 70.

- Verdadeiro - os controladores devem disponibilizar informações sobre como processam os dados pessoais, devem agir como declaram e não enganar os sujeitos dos dados.

19. A conformidade com a proteção de dados por padrão e a proteção de dados por projeto é importante ao avaliar padrões enganosos de projeto, pois isso resultaria em evitá-los em primeiro lugar. De fato, confrontar o serviço e as interfaces associadas aos elementos que compõem a Proteção de Dados por Default e os princípios de Projeto, como os mencionados acima, ajudará a identificar aspectos do serviço que constituiriam um padrão de projeto enganoso antes de lançar o serviço. Por exemplo, se as informações sobre proteção de dados forem fornecidas sem seguir o princípio "No deception", então é provável que constituam um padrão de projeto enganoso de ***Direção Escondida à Clara*** ou ***Emocional*** que será desenvolvido no caso 1.

3 O CICLO DE VIDA DE UMA CONTA DE MÍDIA SOCIAL: COLOCANDO OS PRINCÍPIOS EM PRÁTICA

20. A GDPR se aplica a todo o curso do processamento de dados pessoais por meios automatizados.[21] No caso do processamento de dados pessoais como parte da operação de plataformas de mídia social, isto leva à aplicação da GDPR e seus princípios a todo o ciclo de vida de uma conta de usuário.

3.1 Abertura de uma conta na mídia social

Caso de uso 1: Registro de uma conta

a. Descrição do contexto

21. O primeiro passo que os usuários precisam dar para ter acesso a uma plataforma de mídia social é se inscrever através da criação de uma conta. Como parte deste processo de registro, os usuários são solicitados a fornecer seus dados pessoais, tais como nome e sobrenome, endereço de e-mail ou, às vezes, número de telefone. Os usuários precisam ser informados sobre o processamento de seus dados pessoais e geralmente são solicitados a confirmar que leram o aviso de privacidade e concordam com os termos de uso da plataforma de mídia social. Esta informação precisa ser fornecida em uma linguagem clara e clara, para que os usuários estejam em condições de compreendê-la facilmente e concordem conscientemente.

22. Nesta etapa inicial do processo de inscrição, os usuários devem entender exatamente o que eles assinam, no sentido de que o objeto do acordo entre a plataforma de mídia social e os usuários deve ser descrito da forma mais clara e clara possível.

23. Portanto, a proteção de dados por projeto deve ser levada em conta pelos provedores de mídia social de forma eficaz para proteger os direitos e liberdades das pessoas em questão.[22]

b. Disposições legais relevantes

24. Os provedores de mídia social precisam se certificar de que implementam corretamente os princípios do artigo 5 GDPR ao projetar suas interfaces. Embora a transparência em relação aos sujeitos dos dados seja sempre essencial, este é especialmente o caso na fase de criação de uma conta com uma plataforma de mídia social. Devido à sua posição como controlador ou processador, as plataformas de mídia social devem fornecer as informações aos usuários ao se inscreverem de forma eficiente e sucinta, assim como claramente diferenciadas de outras informações não relacionadas à proteção de dados.[23] Parte das obrigações de transparência dos controladores é informar aos usuários sobre seus direitos, uma das quais é retirar seu consentimento a qualquer momento, se o consentimento for a base legal aplicável.[24]

i. Consentimento fornecido na fase de cadastramento

25. Como os Artigos 4 (11) e 7 GDPR, esclarecido pelo Considerando 32, afirmam, quando o consentimento é escolhido como base legal para o processamento, ele deve ser "*livremente dado, específico, informado e [uma] indicação inequívoca da vontade da pessoa em causa, pela qual ele ou ela, por declaração ou por uma clara ação afirmativa, significa*

[21] Ver artigo 2 (1) GDPR.

[22] Ver Diretrizes 04/2019 sobre Proteção de Dados por Projeto e por Padrão do Artigo 25.
[23] Ver Diretrizes sobre transparência, para. 8.
[24] Diretrizes sobre transparência, para. 30 e página 39.

acordo para o tratamento dos dados pessoais a ele relativos". Todos estes requisitos de consentimento devem ser cumpridos cumulativamente para que sejam considerados como válidos.

26. Para provedores de mídia social que pedem o consentimento dos usuários para diversos fins de processamento, as Diretrizes EDPB 05/2020 sobre consentimento fornecem orientações valiosas sobre a coleta de consentimento.[25] As plataformas de mídia social não devem contornar condições, tais como a capacidade das pessoas em causa de darem livremente o consentimento, através de desenhos gráficos ou redação que impeça as pessoas em causa de exercerem tal vontade. A esse respeito, o Artigo 7 (2) da GDPR estabelece que o pedido de consentimento deve ser apresentado de forma claramente distinguível de outros assuntos, de forma inteligível e facilmente acessível, usando linguagem clara e clara. Os usuários de plataformas de mídia social podem fornecer consentimento para anúncios ou tipos especiais de análise durante o processo de inscrição e, em uma etapa posterior, através das configurações de proteção de dados. Em qualquer caso, como sublinha o considerando 32 GDPR, o consentimento sempre precisa ser dado por um ato afirmativo claro, para que caixas pré-coladas ou inatividade dos usuários não constituam consentimento.[26]

27. Como já destacado pelas Diretrizes da EDPB sobre consentimento, deve haver um mínimo de informação que os usuários recebam para cumprir o limite do consentimento "informado".[27] Se este não for o caso, o consentimento adquirido durante o processo de assinatura não pode ser considerado válido sob a GDPR, tornando assim o processamento ilegal.

28. Os usuários são solicitados a fornecer consentimento para diferentes tipos de finalidades (por exemplo, processamento posterior de dados pessoais). O consentimento não é específico e, portanto, não é válido quando os usuários também não são fornecidos de maneira clara com as informações sobre o que eles estão consentindo. [28] Como prevê o artigo 7 (2) da GDPR, o consentimento deve ser solicitado de forma a distingui-lo claramente de outras informações, não importando como as informações sejam apresentadas ao sujeito dos dados. Em particular, quando o consentimento for solicitado por meios eletrônicos, este consentimento não deve ser incluído nos termos e condições.[29] Considerando o fato de que um número crescente de usuários acessa plataformas de mídia social usando a interface de seus celulares inteligentes para se inscreverem na plataforma, os provedores de mídia social têm que prestar atenção especial à forma como o consentimento é solicitado, para garantir que este consentimento seja distinguível. Os usuários não devem ser confrontados com informações excessivas que os levem a pular a leitura de tais informações. Caso contrário, quando os usuários são "obrigados" a confirmar que leram toda a política de privacidade e concordam com os termos e condições do provedor de mídia social, incluindo todas as operações de processamento, a fim de criar uma conta, isto pode ser qualificado como consentimento forçado às condições especiais ali mencionadas. Se a recusa do consentimento leva à negação do serviço, ele não pode ser considerado tão livremente dado, granularmente e específico, como exige a GDPR. O consentimento que é "agregado" com a aceitação dos termos e condições de um provedor de mídia social não se qualifica como "dado livremente".[30] Este também é o caso quando o controlador "vincula" o fornecimento de um contrato ou um serviço ao pedido de consentimento, de modo que ele processe dados pessoais que não são necessários para a execução do contrato pelo controlador.

29. Embora o consentimento deva ser expresso por uma ação positiva por parte dos usuários, a falta de consentimento deve ser considerada o estado padrão, até que o consentimento tenha sido dado. A expressão da recusa dos usuários

[25] Diretrizes EDPB 05/2020 sobre consentimento sob o Regulamento 2016/679, Versão 1.1., adotado em 4 de maio de 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[26] Ver Tribunal de Justiça da União Européia, Acórdão de 1 de outubro de 2019, *Verbraucherzentrale Bundesverband e.V. v. Planet 49 GmbH*, processo C-673/17, para. 62-63.
[27] Diretrizes 05/2020 sobre consentimento, para. 64; veja também abaixo o caso de uso 3a na parte 3.3. destas Diretrizes.
[28] Ver Diretrizes 05/2020 sobre consentimento, para. 68.
[29] Diretrizes sobre transparência, para. 8.
[30] Ver Diretrizes 8/2020 sobre o direcionamento dos usuários das mídias sociais, para. 57.

não deve, portanto, exigir qualquer ação de sua parte ou deve ser possível através de uma ação que apresente o mesmo grau de simplicidade que a que permite expressar seu consentimento.[31]

ii. Retirada do consentimento - Artigo 7 (3) do GDPR

30. De acordo com a frase 1 do artigo 7 (3) da GDPR, os usuários de plataformas de mídia social poderão retirar seu consentimento a qualquer momento. Antes de dar o consentimento, os usuários também deverão estar cientes do direito de retirar o consentimento, conforme exigido pelo Artigo 7 (3) frase 3 GDPR. Em particular, os controladores deverão demonstrar que os usuários têm a possibilidade de recusar o fornecimento do consentimento ou de retirar o consentimento sem qualquer prejuízo. Os usuários de plataformas de mídia social que consentirem no processamento de seus dados pessoais com um clique, por exemplo, marcando uma caixa, poderão retirar seu consentimento de maneira igualmente fácil.[32] Isto enfatiza que o consentimento deve ser uma decisão reversível, de modo que permaneça um grau de controle para o sujeito dos dados relacionados com o respectivo processamento.[33] A retirada fácil do consentimento constitui um pré-requisito de consentimento válido sob o artigo 7 (3) frase 4 GDPR e deve ser possível sem baixar os níveis de serviço.[34] Como exemplo, o consentimento não pode ser considerado válido sob a GDPR quando o consentimento é obtido através de apenas um clique do mouse, deslizar ou pressionar uma tecla, mas a retirada dá mais passos,[35] é mais difícil de conseguir ou leva mais tempo.

c. Padrões de design enganosos

31. Várias disposições da GDPR dizem respeito ao processo de inscrição. Portanto, há uma série de padrões de design enganosos que podem ocorrer quando os provedores de mídia social não implementam a GDPR como apropriado.

i. Padrões baseados no conteúdo

Sobrecarga - Alerta contínuo (Anexo I lista de verificação 4.1.1)

32. O padrão de projeto ***contínuo e*** enganoso ocorre quando os usuários são pressionados a fornecer mais dados pessoais do que o necessário para fins de processamento ou para concordar com outro uso de seus dados, ao serem repetidamente solicitados a fornecer dados adicionais ou a consentir com um propósito de processamento. Tais solicitações repetitivas podem ocorrer através de um ou vários dispositivos. É provável que os usuários acabem cedendo, pois estão cansados de ter que recusar o pedido cada vez que utilizam a plataforma.

> **Exemplo 1:**
>
> **Variação A:** Na primeira etapa do processo de inscrição, os usuários são obrigados a escolher entre diferentes opções para seu registro. Eles podem fornecer ou um endereço de e-mail ou um número de telefone. Quando os usuários escolhem o endereço de e-mail, o provedor de mídia social ainda tenta convencer os usuários a fornecer o número de telefone, declarando que ele será usado para segurança da conta, sem fornecer alternativas sobre os dados que poderiam ser ou já foram fornecidos pelos usuários. Concretamente,

[31] Ver o considerando 42, frase 5, do GDPR.
[32] Ver Diretrizes sobre transparência, para. 113 e seguintes.

[33] Diretrizes 05/2020 sobre consentimento, para. 10.
[34] Diretrizes 05/2020 sobre consentimento, para. 114.
[35] Ver Diretrizes 05/2020 sobre consentimento, para. 114.

campo para o número de telefone, juntamente com a explicação "*Vamos usar seu número [de telefone] para segurança da conta*". Embora os usuários possam fechar a janela, eles ficam sobrecarregados e desistem ao fornecer seu número de telefone.

Variação B: Outro provedor de mídia social pede repetidamente aos usuários que forneçam o número de telefone toda vez que entram em sua conta, apesar do fato de que os usuários se recusaram a fornecê-lo anteriormente, seja durante o processo de inscrição ou no último

33. O exemplo acima ilustra a situação em que os usuários são continuamente solicitados a fornecer dados pessoais específicos, tais como seu número de telefone. Enquanto na variação A do exemplo, esta ***solicitação contínua*** é feita várias vezes durante o processo de inscrição, a variação B mostra que os usuários também podem ser confrontados com este padrão de design enganoso quando já tiverem se registrado. Para evitar este padrão de design enganoso, é importante estar particularmente atento aos princípios de minimização de dados sob o Artigo 5 (1) (c) GDPR e, em casos como o descrito no exemplo 1 da variação A, também ao princípio de limitação da finalidade sob o Artigo 5 (1) (b) GDPR. Portanto, quando os provedores de mídia social declararem que usarão o número de telefone "para fins de segurança de conta", eles só processarão o número de telefone para tais fins de segurança e não devem processar o número de telefone de uma maneira que vá além deste propósito inicial.

34. Para observar o princípio da minimização de dados, os provedores de mídia social são obrigados a não solicitar dados adicionais, como o número de telefone, quando os usuários de dados já fornecidos durante o processo de cadastramento forem suficientes. Por exemplo, para garantir a segurança da conta, a autenticação aprimorada é possível sem o número de telefone, simplesmente enviando um código para as contas de e-mail dos usuários ou por vários outros meios.

35. Os provedores de redes sociais devem, portanto, contar com meios de segurança que sejam mais fáceis de serem reiniciados pelos usuários. Por exemplo, o provedor de redes sociais pode enviar aos usuários um número de autenticação através de um canal de comunicação adicional, como um aplicativo de segurança, que os usuários instalaram previamente em seu telefone celular, mas sem exigir o número do telefone celular do usuário. A autenticação do usuário via endereço de e-mail também é menos intrusiva do que via número de telefone porque os usuários poderiam simplesmente criar um novo endereço de e-mail especificamente para o processo de inscrição e utilizar esse endereço de e-mail principalmente em conexão com a Rede Social. Um número de telefone, entretanto, não é tão facilmente intercambiável, dado que é altamente improvável que os usuários comprem um novo cartão SIM ou concluam um novo contrato telefônico somente por motivo de autenticação.

36. Deve-se ter em mente que se o objetivo de tal pedido é provar que os usuários estão legitimamente na posse do dispositivo utilizado para entrar na rede social, este objetivo pode ser alcançado por vários meios, sendo que um número de telefone é apenas um deles. Assim, um número de telefone só pode constituir uma opção relevante, numa base voluntária para os usuários. Finalmente, os usuários precisam decidir se desejam utilizar este meio como um fator de autenticação. Em particular, para uma verificação única, os números de telefone dos usuários não são necessários porque o endereço de e-mail constitui o ponto de contato regular com os usuários durante o processo de registro.

37. A prática ilustrada no exemplo 1 variação A pode enganar os usuários e levá-los a fornecer tais informações de má vontade, acreditando que isso é necessário para ativar ou proteger a conta. Entretanto, na realidade, nunca foi fornecida aos usuários a alternativa (por exemplo, o uso do e-mail para fins de ativação da conta e segurança). No exemplo 1 variante B, os usuários não são

informados sobre um propósito de processamento. No entanto, esta variação ainda constitui um padrão de design enganoso ***contínuo***, pois o provedor de mídia social desconsidera o fato de que os usuários anteriormente se recusavam a fornecer o telefone

número, e continua pedindo por ele. Quando os usuários têm a impressão de que só podem evitar este pedido repetido inserindo seus dados, é provável que cedam.

38. No exemplo a seguir, os usuários são repetidamente encorajados a dar à plataforma de mídia social acesso a seus contatos:

> **Exemplo 2:** Uma plataforma de mídia social usa uma informação ou um ícone de ponto de interrogação para incitar os usuários a tomar a ação "opcional" atualmente solicitada. Entretanto, ao invés de apenas fornecer informações aos usuários que esperam ajuda desses botões, a plataforma solicita aos usuários que aceitem importar seus contatos de sua conta de e-mail, mostrando repetidamente um pop-up dizendo "Vamos *fazer isso*".

39. Particularmente na etapa do processo de inscrição, este ***Prompting Contínuo*** pode influenciar os usuários a simplesmente aceitar o pedido da plataforma a fim de finalmente completar seu registro. O efeito deste padrão de design enganoso é acentuado quando combinado com linguagem motivacional como neste exemplo, acrescentando um senso de urgência.

40. Os efeitos de influência da redação e do visual serão abordados mais adiante, ao examinar o padrão de design enganoso ***Direção Emocional***.[36]

Obstrução - Ação enganosa (Anexo I lista de verificação 4.4.3)

41. Outro exemplo de uma situação em que os provedores de mídia social pedem os números de telefone dos usuários sem necessidade diz respeito ao uso do aplicativo da plataforma:

> **Exemplo 3:** Ao se registrar em uma plataforma de mídia social via navegador de desktop, os usuários são convidados a usar também a aplicação móvel da plataforma. Durante o que parece ser mais um passo no
> processo de inscrição, os usuários são convidados a descobrir o aplicativo. Ao clicar no ícone, esperando ser encaminhados a uma loja de aplicativos, eles são convidados a

42. Explicar aos usuários que eles precisam fornecer o número de telefone para receber um link para baixar o aplicativo constitui uma ***ação enganosa*** por uma série de razões: Em primeiro lugar, existem várias maneiras para os usuários usarem um aplicativo, por exemplo, escaneando um código QR, usando um link ou baixando o aplicativo da loja para aplicativos. Em segundo lugar, estas alternativas mostram que não há nenhuma razão obrigatória para o provedor da plataforma social pedir o número de telefone do usuário. Quando os usuários tiverem concluído o processo de inscrição, eles precisam ser capazes de usar seus dados de login (ou seja, geralmente endereço de e-mail e senha) para efetuar o login, independentemente do dispositivo que estão usando, quer usem um navegador desktop ou móvel ou um aplicativo. Isto é ainda mais sublinhado pelo fato de que, ao invés de um smartphone, os usuários poderiam desejar instalar o aplicativo em seu tablet, que não está vinculado a um número de telefone.

Agitação - Direção emocional (Anexo I lista de verificação 4.3.1)

43. Com o padrão de design enganoso ***Emocional Steering***, as palavras ou elementos visuais (como estilo, cores, imagens ou outros) são utilizados de forma a transmitir informações aos usuários, seja numa perspectiva altamente positiva, fazendo com que os usuários se sintam bem, seguros ou recompensados, ou uma perspectiva altamente negativa, fazendo com que os usuários se sintam

ansiosos, culpados ou punidos. A maneira pela qual a informação é apresentada aos usuários influencia sua

[36] Ver parágrafo. 43 e seguintes no caso 1, assim como a visão geral de exemplos na lista de verificação do Anexo.

estado emocional de uma forma que possa levá-los a agir contra seus interesses de proteção de dados. Os impactos de tais práticas podem ser ainda mais eficazes se forem baseados em dados coletados pela plataforma. Influenciar decisões fornecendo informações tendenciosas aos indivíduos pode geralmente ser considerado como uma prática desleal contrária ao princípio de justiça de processamento estabelecido no Artigo 5 (1) (a) GDPR. Ela pode ocorrer durante toda a jornada do usuário dentro de uma plataforma de mídia social. Entretanto, na fase de inscrição, o efeito de direção pode ser especialmente forte, considerando a sobrecarga de informações que os usuários podem ter que lidar além das etapas necessárias para completar o registro.

44. luz do exposto acima, a ***Direção Emocional*** na fase de registro em uma plataforma de mídia social pode ter um impacto ainda maior nas crianças, idosos e outros grupos (ou seja, fornecer mais dados pessoais devido à falta de compreensão das atividades de processamento), considerando sua natureza vulnerável como sujeitos de dados.[37] Quando os serviços da plataforma de mídia social são dirigidos a crianças ou outros indivíduos vulneráveis, eles devem assegurar que a linguagem utilizada, incluindo seu tom e estilo, seja apropriada para que os usuários vulneráveis, como destinatários da mensagem, compreendam facilmente as informações fornecidas.[38] Considerando a vulnerabilidade de crianças, idosos e outros sujeitos de dados, padrões de design enganosos podem influenciar esses usuários a compartilhar mais informações, pois expressões "imperativas" podem fazê-los sentir-se obrigados a fazê-lo, por exemplo, para parecerem populares entre os pares ou porque acreditam que o fornecimento dos dados é obrigatório.

45. Quando os usuários de plataformas de mídia social são solicitados a entregar seus dados rapidamente, eles não têm tempo para "processar" e assim compreender realmente as informações que lhes são fornecidas, a fim de tomar uma decisão consciente. A linguagem motivacional utilizada pelas plataformas de mídia social poderia encorajar os usuários a fornecer posteriormente mais dados do que os necessários, quando eles sentem que o que é proposto pela plataforma de mídia social é o que a maioria dos usuários fará e, portanto, a "forma correta" de proceder.

> **Exemplo 4:** A plataforma de mídia social pede aos usuários que compartilhem sua geolocalização, declarando: "Ei, um lobo solitário, você é? Mas compartilhar e conectar-se com outros ajuda a tornar o mundo um lugar melhor! Compartilhe sua geolocalização!

46. Durante o processo de inscrição, o objetivo dos usuários é completar o registro para poder utilizar a plataforma de mídia social. Padrões de design enganosos como o ***Emotional Steering*** têm efeitos mais fortes neste contexto. Estes correm o risco de serem mais fortes no meio ou no final do processo de inscrição em comparação com o início, já que os usuários na maioria das vezes completam todas as etapas necessárias "com pressa", ou são mais suscetíveis a um senso de urgência. Neste contexto, é mais provável que os usuários aceitem colocar todos os dados que são solicitados a fornecer, sem tomar o tempo necessário para questionar se devem fazê-lo. Neste sentido, a linguagem motivacional utilizada pelo fornecedor de mídia social pode ter influência na decisão imediata dos usuários, assim como a combinação da linguagem motivacional com outras formas de ênfase, tais como pontos de exclamação, como mostrado no exemplo abaixo.

> **Exemplo 5: O** provedor de mídia social incentiva os usuários a incentivá-los a compartilhar mais dados pessoais do que os realmente necessários, solicitando aos usuários que forneçam uma auto-descrição: "*Conte-nos sobre seu incrível self! Não podemos esperar,*

47. Com esta prática, as plataformas de mídia social recebem um perfil mais detalhado de seus usuários. Entretanto, dependendo do caso, fornecer mais dados pessoais, por exemplo, relativos à personalidade dos usuários, pode não ser necessário para o uso do serviço em si e, portanto, violar o

princípio da minimização de dados, conforme o Artigo 5 (1) (c) GDPR. Como ilustrado no exemplo 5, tais técnicas não cultivam o livre arbítrio dos usuários para

[37] Ver também acima, para. 7.
[38] Ver Diretrizes sobre transparência, para. 18.

fornecer seus dados, uma vez que a linguagem prescritiva utilizada pode fazer com que os usuários se sintam obrigados a fornecer uma autodescrição, pois eles já dedicaram tempo ao registro e desejam completá-lo. Quando os usuários estão em processo de registro para uma conta, é menos provável que eles demorem tempo para considerar a descrição que dão ou mesmo se gostariam de dar uma. Este é particularmente o caso quando a linguagem utilizada proporciona um senso de urgência ou soa como um imperativo. Se os usuários sentirem esta obrigação, mesmo quando na realidade o fornecimento dos dados não é obrigatório, isto pode ter um impacto em seu "livre arbítrio". Isso também significa que as informações fornecidas pela plataforma de mídia social não eram claras.

> **Exemplo 6:** A parte do processo de inscrição onde os usuários são solicitados a carregar sua foto contém um botão "?". Clicando nele revela a seguinte mensagem: "*Não há necessidade de ir primeiro ao cabeleireiro". Basta escolher uma foto que diga 'este sou*

48. Mesmo que as frases do exemplo 6 visem motivar os usuários e aparentemente simplificar o processo por eles (ou seja, sem necessidade de uma foto formal para se inscrever), tais práticas podem ter impacto na decisão final tomada pelos usuários que inicialmente decidiram não compartilhar uma foto para sua conta. Os pontos de interrogação são usados para perguntas e, como um ícone, os usuários podem esperar encontrar informações úteis ao clicar sobre elas. Quando esta expectativa não for atendida e os usuários forem solicitados mais uma vez a tomar a ação sobre a qual estão hesitantes, o consentimento coletado sem informar os usuários sobre o processamento de sua foto não seria válido, não cumprindo os requisitos de consentimento "informado" e "dado livremente" sob o Artigo 7 GDPR em conjunto com o Artigo 4 (11) GDPR. O fator emocional, portanto, tem uma forte influência sobre a legitimidade do consentimento.

Obstrução - Mais longa do que o necessário (Anexo I lista de verificação 4.4.2)

49. Quando os usuários tentam ativar um controle relacionado à proteção de dados, mas a jornada do usuário é feita de uma forma que requer que os usuários completem mais etapas, em comparação com o número de etapas necessárias para a ativação de opções invasivas de dados, isto constitui o padrão de projeto enganoso ***Mais tempo do que o necessário.*** Este padrão provavelmente desencoraja os usuários de ativar os controles de proteção de dados. No processo de inscrição, isto pode se traduzir na exibição de uma janela pop-in ou pop-up pedindo aos usuários que confirmem sua decisão quando escolherem uma opção restritiva (por exemplo, optando por tornar seus perfis privados). O exemplo abaixo ilustra outro caso em que um processo de cadastramento é ***mais longo do que o necessário.***

> **Exemplo 7:** Durante o processo de inscrição, os usuários que clicam nos botões "pular" para evitar a entrada de certos tipos de dados são mostrados uma janela pop-up perguntando "*Você tem certeza?* Questionando sua decisão e, portanto, fazendo-os duvidar dela, o provedor de mídia social incita os usuários a analisá-la e divulgar este tipo de dados, tais como seu sexo, lista de contatos ou foto. Em contraste, os usuários que optam por inserir diretamente os dados não vêem nenhuma mensagem pedindo para reconsiderar sua

Aqui, pedir aos usuários a confirmação de que não querem preencher um campo de dados pode fazê-los voltar atrás em sua decisão inicial e inserir os dados solicitados. Este é particularmente o caso dos usuários que não estão familiarizados com as funções da plataforma de mídia social. Este padrão de projeto ***mais longo do que o necessário*** tenta influenciar as decisões dos usuários, retendo-os e questionando sua escolha inicial, além de prolongar desnecessariamente o processo

de inscrição, o que constitui uma violação do princípio de justiça sob o Artigo 5 (1) (a) GDPR. O exemplo mostra que o padrão de design enganoso pode levar os usuários a revelar (mais) dados pessoais do que eles inicialmente escolheram. Ele descreve um desequilíbrio de tratamento dos usuários que divulgam dados pessoais imediatamente e daqueles que não o fazem: Somente aqueles que se recusam a revelar os dados são solicitados a confirmar sua escolha, enquanto os usuários que revelam os dados não são solicitados a confirmar sua escolha. Isto constitui uma violação da justiça.

de acordo com o artigo 5 (1) (a) GDPR em relação aos usuários que não desejam divulgar esses dados pessoais.

ii. Padrões baseados em interfaces

Agitação - Escondido em plena vista (Anexo I lista de verificação 4.3.2)

50. De acordo com o princípio de transparência, as pessoas interessadas devem receber informações de maneira clara para que possam entender como seus dados pessoais são processados e como podem controlá-los. Além disso, essas informações devem ser facilmente percebidas pelas pessoas em questão. No entanto, as informações relacionadas à proteção de dados, em particular links, são freqüentemente exibidas de tal forma que os usuários as ignorarão facilmente. Tais práticas de ***Escondido à vista de todos*** utilizam um estilo visual para informações ou controles de proteção de dados que afasta os usuários das opções vantajosas de proteção de dados para opções menos restritivas e, portanto, mais invasivas.

51. O uso de fontes de tamanho pequeno ou uma cor que não contraste o suficiente para oferecer suficiente legibilidade (por exemplo, cor de texto cinza fraco sobre um fundo branco) pode ter impacto negativo nos usuários, pois o texto será menos visível e os usuários ou o negligenciarão ou terão dificuldades para lê-lo. Este é especialmente o caso quando um ou mais elementos atraentes são colocados ao lado das informações obrigatórias relacionadas à proteção de dados. Estas técnicas de interface enganam os usuários e tornam a identificação das informações relacionadas à sua proteção de dados mais onerosa e demorada, pois requer mais tempo e minúcia para detectar as informações relevantes.

> **Exemplo 8:** Imediatamente após completar o registro, os usuários só podem acessar informações de proteção de dados chamando o menu geral da plataforma de mídia social e navegando na seção de submenu que inclui um link para "*privacidade e configurações de dados*". Após uma visita a esta página, um link para a política de privacidade não é visível à primeira vista. Os usuários têm que notar, em um canto da página, um pequeno ícone apontando para a política de privacidade, o que significa que os usuários dificilmente

52. É importante observar que mesmo quando os provedores de mídia social disponibilizam todas as informações a serem fornecidas aos sujeitos dos dados sob os Artigo 13 e 14 GDPR, a forma como essas informações são apresentadas ainda pode infringir as exigências abrangentes de transparência sob o Artigo 12 (1) GDPR. Quando a informação é ***ocultada à vista de todos*** e, portanto, é provável que seja ignorada, isto leva a confusão ou desorientação e não pode ser considerado inteligível e facilmente acessível, contrariamente ao Artigo 12 (1) GDPR.

53. Embora o exemplo acima mostre o padrão de design enganoso após a conclusão do processo de inscrição, este padrão também já ocorre durante o processo de inscrição, como será mostrado no exemplo ilustrado abaixo, que combina os padrões ***Escondido à vista*** e ***Aconchego Enganoso.***

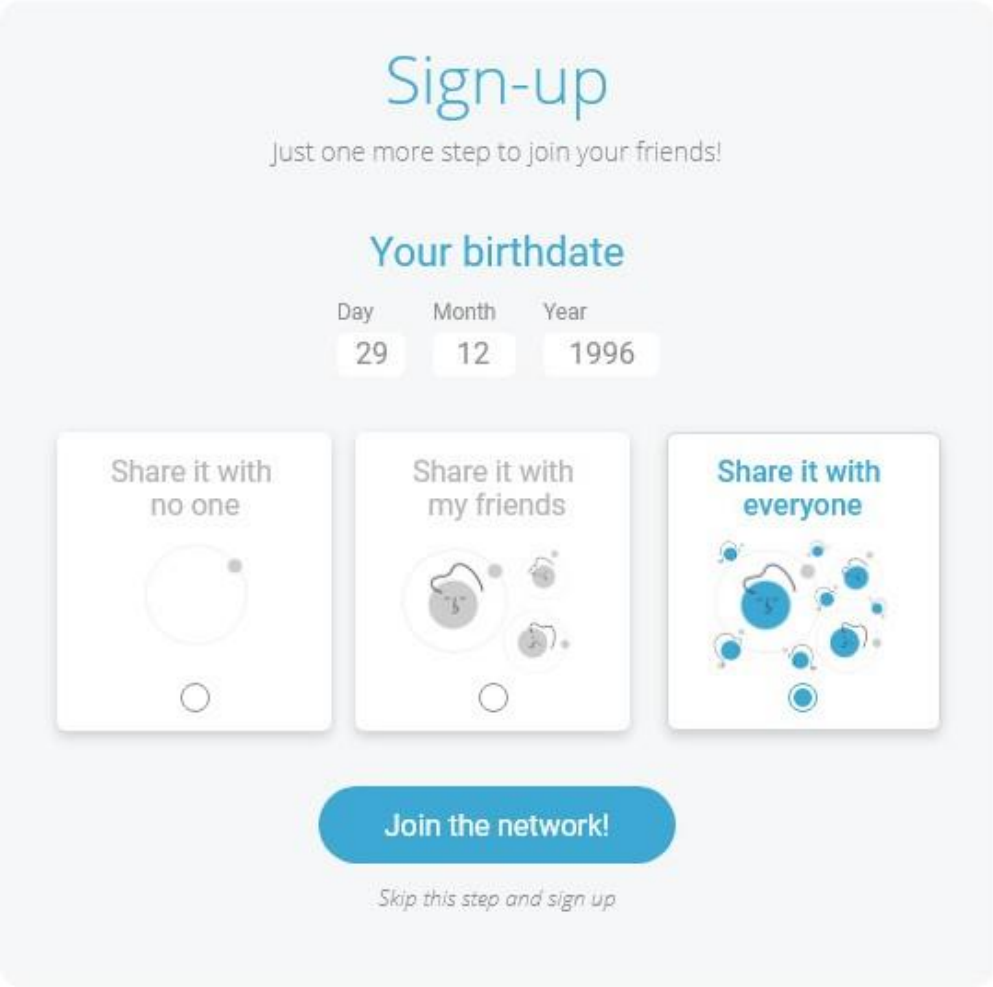
Pular - Aconchego enganoso (Anexo I lista de verificação 4.2.1)

54. Os provedores de mídia social também precisam estar atentos ao princípio de proteção de dados por padrão. Quando as configurações de dados são pré-selecionadas, os usuários estão sujeitos a um nível específico de proteção de dados, determinado pelo provedor por padrão, e não pelos usuários.

Além disso, os usuários nem sempre têm a opção imediata de alterar as configurações para configurações mais rígidas e compatíveis com a proteção de dados. A conformidade com a GDPR a este respeito não significa que todas as opções precisam ter exatamente a mesma aparência. Entretanto, se as opções sociais

Os provedores de mídia destacam uma das opções e, portanto, chamam a atenção dos usuários para ela, esta deve ser a mais restritiva em relação aos dados pessoais, a fim de cumprir, entre outras coisas, o princípio da minimização de dados nos termos do Artigo 5 (1) (c) GDPR.

55. Quando as características e opções mais invasivas de dados são ativadas por padrão, isto constitui o padrão de ***Aconchego Enganoso***. Por causa do efeito padrão que impele os indivíduos a manter uma opção pré-selecionada, é improvável que os usuários a alterem, mesmo que seja dada a possibilidade. Esta prática é comumente encontrada em processos de inscrição, como ilustrado no exemplo 9 abaixo, pois é uma forma eficaz de ativar opções invasivas de dados que os usuários provavelmente recusariam de outra forma. Tais padrões de design enganosos entram em conflito com o princípio de proteção de dados por default do Artigo 25 (2) GDPR, especialmente quando afetam a coleta de dados pessoais, a extensão do processamento, o período de armazenamento de dados e a acessibilidade dos dados.[39]



Exemplo 9: Neste exemplo, quando os usuários entram com sua data de nascimento, eles são convidados a escolher com quem compartilhar estas informações. Enquanto opções menos invasivas estão disponíveis, a opção *"compartilhar com todos"* é selecionada por padrão, o que significa que todos, ou seja, usuários registrados, assim como qualquer

[39] Veja também para. 446 da Decisão Final da Autoridade Irlandesa de Proteção de Dados referente à Instagram (Meta Platforms Ireland Limited) após a decisão vinculativa de resolução de disputas da EDPB de 28 de julho de

2022, https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_en.

56. O exemplo 9 mostra um padrão de ***Snugness Deceptive***, pois não é a opção que oferece o mais alto nível de proteção de dados que é selecionada, e portanto ativada, por padrão. Além disso, o efeito padrão deste padrão impele os usuários a manter a pré-seleção, ou seja, a não levar tempo para considerar as outras opções nesta etapa, nem para voltar a alterar a configuração em uma etapa posterior. O padrão ***Hidden in Plain Sight*** também é usado nesta interface. De fato, a entrada da data de nascimento não é obrigatória, pois os usuários podem pular esta etapa de inscrição clicando no link *"Pular esta etapa e inscrever-se"* que está disponível abaixo do botão *"Junte-se à rede! O* fato de que o campo de data de nascimento e o botão de confirmação são tão proeminentes é provável que impeça os usuários a inserir sua data de nascimento e enviá-la para a rede social porque eles não percebem a possibilidade de não compartilhar esta informação. Este efeito seria ainda mais forte se círculos animados fossem utilizados junto ao campo e ao botão que atraem fortemente a atenção dos usuários.

57. Respeitar o princípio de proteção de dados por projeto e padrão não significa que todas as opções oferecidas precisam parecer exatamente as mesmas. Entretanto, se os controladores decidirem destacar uma opção mais do que a(s) outra(s), a opção destacada precisa ser a mais restritiva em relação ao processamento de dados.

58. Além de incitar os usuários a manter uma opção que não corresponde necessariamente às suas preferências, os provedores de mídia social podem não incitar os usuários a verificar ou modificar suas configurações de proteção de dados de acordo com suas preferências após concluir o processo de inscrição. Além disso, a alteração dessas configurações padrão pode exigir várias etapas. Quando os usuários não são de forma alguma solicitados a verificar ou modificar suas configurações de proteção de dados ou não são direcionados de forma clara a qualquer informação relacionada, seu nível de proteção de dados dependerá de sua própria iniciativa. Para facilitar o controle dos usuários sobre seus dados, podem ser usados os chamados painéis de controle de privacidade que são projetados para centralizar e facilitar tal esforço.

59. É importante ter em mente que a falta de proteção de dados por projeto e padrão, em combinação com o efeito padrão acima mencionado, pode ter conseqüências prejudiciais para os sujeitos dos dados, inclusive para sua segurança cibernética. A exibição pública de dados pessoais, como a data de nascimento, que é utilizada para processos de verificação por outros serviços on-line, poderia facilitar o acesso dos criminosos às compras dos usuários, aos bancos e a outras contas. Outra conseqüência prejudicial diz respeito às possibilidades de contato na plataforma de mídia social: se a opção padrão para enviar solicitações de contato ou mensagens aos usuários for definida para "qualquer pessoa", isto aumenta o risco de ciberrooming e fraude, especialmente em grupos vulneráveis.

60. Finalmente, quando o ***Aconchego Enganoso*** é aplicado à coleta de consentimento, o que equivaleria a considerar o consentimento dos usuários por padrão, por exemplo, usando uma caixa pré-colada ou considerando a inatividade como aprovação, as condições para consentimento estabelecidas no Artigo 4 (11) GDPR não são cumpridas e o processamento seria considerado ilegal sob os Artigos 5 (1) (a) e 6 (1) (a) GDPR.

Obstrução - Ponto morto (Anexo I lista de verificação 4.4.1)

61. É importante ressaltar que a etapa do processo de inscrição é um momento decisivo para que os usuários se informem. Se eles estão procurando informações e não conseguem encontrá-las, pois

não há um link de redirecionamento disponível ou funcionando, isto constitui um padrão de Beco ***sem saída***, pois os usuários ficam impossibilitados de atingir este objetivo.

> **Exemplo 10:** Não são fornecidos aos usuários quaisquer links para informações sobre proteção de dados uma vez iniciado o processo de inscrição. Os usuários não podem encontrar estas informações, pois nenhuma é fornecida em nenhum lugar na interface de cadastramento,

62. Na prática, este exemplo implica que os usuários só poderão parar o registro e voltar para a página inicial se esta contiver um link para a nota de privacidade, ou para completar o registro, fazer o login para

a plataforma de mídia social e somente então ter acesso às informações relacionadas à proteção de dados. Isto infringe o princípio de transparência e fácil acesso às informações que os sujeitos dos dados devem receber, conforme exigido no artigo 12 (1) da GDPR. Também não atende às exigências do Artigo 13 (1) e (2) da GDPR, pois nenhuma informação é fornecida e acessível no momento em que os dados pessoais são obtidos.

63. O padrão ***Dead end*** também pode ocorrer de outra forma quando os usuários recebem uma ação ou opção relacionada à proteção de dados durante o processo de inscrição que não podem encontrar novamente mais tarde, enquanto utilizam o serviço.

> **Exemplo 11:** Durante o processo de registro, os usuários podem consentir no processamento de seus dados pessoais para fins publicitários e são informados de que podem mudar sua escolha sempre que quiserem, uma vez registrados nas mídias sociais, indo para a política de privacidade.
> No entanto, uma vez que os usuários tenham concluído o processo de registro e tenham

64. Neste exemplo específico, os usuários não têm meios de retirar seu consentimento uma vez inscrito. Aqui, o padrão de desenho enganoso O ***beco sem saída*** infringe o direito das pessoas em questão de retirar o consentimento a qualquer momento, e tão facilmente quanto dar o consentimento, sob as frases 1 e 4 do Artigo 7 (3) GDPR.

65. Finalmente, apontar os usuários para um link que supostamente os leva a páginas relacionadas à proteção de dados, tais como configurações ou informações de proteção de dados, também é um exemplo de um padrão de ***beco sem saída*** se o link for quebrado e não forem disponibilizados links de retorno que ajudem os usuários a encontrar o que eles estão procurando. Desta forma, os usuários não podem procurar as informações relevantes, enquanto não lhes são fornecidas explicações, como a razão pela qual isto ocorre (por exemplo, questões técnicas). Em tal caso, as mesmas questões relacionadas à transparência e fácil acesso à informação, conforme descrito no parágrafo. 58 ocorrem.

d. As melhores práticas

Para projetar interfaces de usuário que facilitem a implementação efetiva da GDPR, a EDPB recomenda a implementação das seguintes melhores práticas para o processo de inscrição:

> **Atalhos**: Links para informações, ações ou configurações que possam ser de ajuda prática aos usuários para gerenciar seus dados e suas configurações de proteção de dados devem estar disponíveis onde quer que eles sejam confrontados com informações ou experiências relacionadas (por exemplo, *links redirecionando para as partes relevantes da política de privacidade*).
>
> **Informações de contato**: O endereço de contato da empresa para tratar dos pedidos de proteção de dados deve ser claramente indicado na política de privacidade. Deve estar presente em uma seção onde os usuários podem esperar encontrá-lo, como uma seção sobre a identidade do controlador dos dados, uma seção relacionada aos direitos ou uma seção de contato.
>
> **Chegar à autoridade supervisora**: Declarar a identidade específica da autoridade fiscalizadora e incluir um link para seu website ou para a página específica do website relacionada com a apresentação de uma reclamação. Esta informação deve estar presente em uma seção onde os usuários podem esperar encontrá-la, como uma seção relacionada a direitos.
>
> **Visão geral da Política de Privacidade**: No início / topo da política de privacidade, inclua um índice (dobrável) com títulos e subtítulos que mostrem as diferentes passagens que a nota de privacidade contém. Os nomes das passagens individuais conduzem claramente os usuários quanto ao conteúdo exato e permitem que eles identifiquem rapidamente e saltem para a seção que estão procurando.

Palavras coerentes: Em todo o site, a mesma formulação e definição é usada para a mesma proteção de dados. A redação usada na política de privacidade deve corresponder à usada no resto da plataforma.

Fornecendo definições: Ao utilizar palavras ou jargões não familiares ou técnicos, fornecer uma definição em linguagem simples ajudará os usuários a compreender as informações fornecidas a eles. A definição pode ser dada diretamente no texto, quando os usuários pairam sobre a palavra, bem como ser disponibilizada em um glossário.

Elementos contrastantes de proteção de dados: Fazer com que elementos ou ações relacionadas à proteção de dados sejam visualmente marcantes em uma interface que não é diretamente dedicada ao assunto. Por exemplo, ao postar uma mensagem pública na plataforma, os controles sobre a associação da geolocalização devem estar diretamente disponíveis e claramente visíveis.

Proteção de dados a bordo: Logo após a criação de uma conta, inclua pontos de proteção de dados dentro da experiência de onboarding do provedor de mídia social para que os usuários descubram e definam suas preferências sem problemas. Por exemplo, isto pode ser feito convidando-os a definir suas preferências de proteção de dados após adicionar seu primeiro amigo ou compartilhar seu primeiro posto.

Uso de exemplos: Além das informações obrigatórias que indicam clara e precisamente o objetivo do processamento, exemplos podem ser usados para ilustrar um processamento de dados específico para torná-lo mais tangível para os usuários.

Informação contextual: além de uma política de privacidade exaustiva, traga pequenos pedaços de informação no momento mais apropriado para que o usuário tenha uma informação específica e contínua sobre como seus dados são processados.

3.2 Mantendo-se informado sobre as mídias sociais

Use o caso 2a: Um aviso de privacidade em camadas

a. **Descrição do contexto**

66. Como já destacado nas Diretrizes sobre transparência, o princípio da transparência está muito ligado ao princípio do tratamento justo dos dados pessoais.[40] Entretanto, as informações sobre o processamento de dados pessoais também fazem com que os controladores de dados reflitam sobre suas próprias ações, tornam o processamento de dados mais compreensível para as pessoas em questão e, em última instância, permitem que as pessoas em questão tenham controle sobre seus dados, especialmente através do exercício de seus direitos. A resultante equalização das capacidades das pessoas envolvidas leva a um sistema justo de processamento de dados pessoais. No entanto, mais informação não significa necessariamente melhor informação. Muitas informações irrelevantes ou confusas podem obscurecer pontos importantes de conteúdo ou reduzir a probabilidade de encontrá-los. Portanto, o equilíbrio correto entre conteúdo e apresentação compreensível é crucial nesta área. Se este equilíbrio não for alcançado, podem ocorrer padrões de design enganosos.

b. **Disposições legais relevantes**

67. As relações que acabamos de delinear tornam-se claras com base no artigo 5 GDPR. Transparência e justiça já são sistematicamente mencionadas lado a lado no Artigo 5 (1) (a) GDPR, já que um componente determina o outro. O fato de que não somente a transparência externa, mas também interna deve existir, também é esclarecido pela exigência de prestação de contas prevista no Artigo 5 (2) GDPR. A parte mais importante da transparência interna é a exigência de manter um registro das

atividades de processamento sob o Artigo 30 da GDPR. Para

[40] Diretrizes sobre transparência, p. 4-5.

transparência externa, os provedores de mídia social podem fornecer um aviso de privacidade em camadas aos usuários, entre outros meios de informação.[41] Esta necessidade de compreensão e processamento justo também resulta nas exigências do Artigo 12 (1) GDPR, que estabelece que qualquer informação referida nos Artigos 13 e 14 GDPR deve ser fornecida de forma concisa, transparente, inteligível e facilmente acessível, usando linguagem clara e clara. Conseqüentemente, o conteúdo da informação deve ser disponibilizado sem obstáculos. Se as exigências do artigo 12 da GDPR não forem cumpridas, não há informações válidas na acepção dos artigos 13 e 14 da GDPR. Assim, para um controle efetivo, os controladores e processadores podem ser responsabilizados, levando à eficácia das exigências da GDPR na prática.

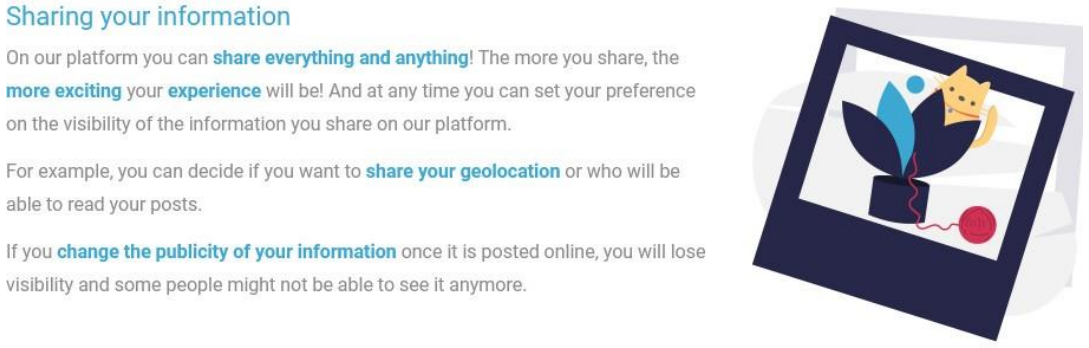
c. Padrões de design enganosos

i. Padrões baseados no conteúdo

68. Com relação a este caso de uso, os padrões baseados no conteúdo encontram seus limites no Artigo 12 (1) GDPR, que exige uma forma precisa e inteligível, bem como uma linguagem clara e clara com relação às informações fornecidas.

Esquerda no escuro - Informações conflitantes (Anexo I lista de verificação 4.6.2)

69. Um dos casos mais óbvios em que isso pode ocorrer é quando são fornecidas ***informações conflitantes***, o que deixa os usuários inseguros do que devem fazer e das conseqüências de suas ações, portanto não tomar nenhuma, ou manter as configurações padrão.



Exemplo 12: Neste exemplo, as informações relacionadas ao compartilhamento de dados dão uma perspectiva altamente positiva do processamento, destacando os benefícios de compartilhar o maior número possível de dados. Juntamente com a ilustração que representa a fotografia de um animal bonito brincando com uma bola, esta ***Direção Emocional*** pode dar aos usuários a ilusão de segurança e conforto com relação aos riscos potenciais de compartilhar algum tipo de informação sobre a plataforma. Por outro lado, as informações dadas sobre como controlar a publicidade de seus dados não são claras. Primeiro, diz-se que os usuários podem definir sua preferência de compartilhamento sempre que quiserem. Depois, porém, a última frase indica que isto não é possível uma vez que algo já tenha sido publicado na plataforma. Essas ***informações conflitantes*** deixam os

[41] Ver Caso de uso 2.a na seção 3.2 abaixo.

Fickle - Falta de Hierarquia (Anexo I lista de verificação 4.5.1)

71. Efeitos similares aos das ***Informações Conflituosas*** e da ***Direção Emocional*** podem ocorrer se a apresentação das informações não seguir um sistema interno ou qualquer hierarquia. Informações relacionadas à proteção de dados que é ***Hierarquia Ausente*** ocorrem quando tais informações aparecem várias vezes e são apresentadas de várias maneiras diferentes. É provável que os usuários fiquem confusos com esta redundância e fiquem impossibilitados de entender completamente como seus dados são processados e como exercer controle sobre eles. Tal arquitetura torna a informação difícil de entender, pois o quadro completo não é facilmente acessível. Em casos como o descrito no exemplo a seguir, isto infringe as exigências de inteligibilidade e facilidade de acesso nos termos do Artigo 12 (1) GDPR.

> **Exemplo 13:** As informações relacionadas aos direitos dos sujeitos dos dados são divulgadas na nota de privacidade.
>
> Embora diferentes direitos sobre os dados sejam explicados na seção "*Suas opções*", o direito de apresentar uma reclamação e o endereço exato de contato é indicado somente após várias seções e camadas referentes a diferentes tópicos. O aviso de privacidade,

72. ***A falta de Hierarquia*** também pode surgir quando a informação dada é estruturada de uma forma que dificulta a orientação dos usuários, como mostra o exemplo a seguir.

> **Exemplo 14:** A política de privacidade não está dividida em diferentes seções com manchetes e conteúdo. São fornecidas mais de 70 páginas. Entretanto, não há um menu de navegação ao lado ou no topo para permitir que os usuários acessem facilmente a seção que estão procurando. A explicação do termo autocriado *"dados de criação"* está contida em uma

Esquerda na Escuridão - Escrita ou Informação Ambígua (Anexo I lista de verificação 4.6.3)

73. Mesmo que a escolha das palavras não seja abertamente contraditória, podem surgir problemas com o uso de termos ambíguos e vagos ao dar informações aos usuários. Com tais informações, os usuários provavelmente ficarão inseguros sobre como os dados serão processados ou como ter algum controle sobre os dados. Se for possível assumir que usuários médios não compreenderiam a mensagem genuína da informação sem conhecimento especial, as condições do Artigo 12 (1) GDPR não são cumpridas. Por extensão, o uso de ***palavras ou informações ambíguas*** pode contradizer o princípio de justiça do Artigo 5 (1) (a) GDPR, uma vez que a informação não pode ser considerada transparente, tornando os sujeitos dos dados incapazes de compreender o processamento de seus dados pessoais e de exercer seus direitos.

> **Exemplo 15:** Uma nota de privacidade descreve parte de um processamento de forma vaga e imprecisa, como nesta frase: "*Seus dados podem ser usados para melhorar nossos serviços*". Além disso, o direito de acesso aos dados pessoais é aplicável ao processamento com base no Artigo 15 (1) GDPR, mas é mencionado de tal forma que não fica claro para os usuários o que ele permite que eles acessem: *"Você pode ver uma parte de suas informações em sua conta e ao rever o que você postou na plataforma".*

74. No exemplo, o uso do tempo condicional ("*poderia*") deixa os usuários inseguros se seus dados serão usados para o processamento ou não. É provável que o termo *"serviços"* seja geral demais para ser qualificado como "claro". Além disso, não está claro como os dados serão processados para a

melhoria dos serviços. A EDPB lembra que o uso de palavras tensas ou vagas condicionadas não constitui "linguagem clara e clara", pois

exigido pelo Artigo 12 (1) frase 1 GDPR e só pode ser usado se os controladores forem capazes de demonstrar que isso não prejudica a justiça do processamento.[42]

Fickle - Descontinuidade do idioma (Anexo I lista de verificação 4.5.4)

75. Quando serviços on-line são oferecidos e dirigidos aos residentes de certos Estados-Membros, os avisos de proteção de dados também devem ser oferecidos nestes idiomas.[43] Neste contexto, é importante que a escolha de um determinado idioma também possa ser trocada manualmente e seja implementada continuamente, sem interrupções. Se estes critérios não forem cumpridos, os sujeitos dos dados serão confrontados com uma ***Descontinuidade de Idioma***, deixando-os incapazes de compreender as informações relacionadas à proteção de dados. Os usuários enfrentarão este padrão de projeto enganoso quando as informações sobre proteção de dados não forem fornecidas nos idiomas oficiais do país onde moram, enquanto que o serviço é fornecido nesse idioma. Se os usuários não dominarem o idioma no qual as informações sobre proteção de dados são fornecidas, não poderão lê-las facilmente e, portanto, não estarão cientes de como seus dados pessoais são processados. É importante observar que a ***Descontinuidade do Idioma*** pode confundir os usuários e criar um ambiente de configuração que eles não entendem como fazer uso. Este padrão de design enganoso pode aparecer de várias maneiras, como será mostrado ao longo destas Diretrizes.

Exemplo 16:

Variação A: A plataforma de mídia social está disponível em croata como o idioma de escolha dos usuários (ou em espanhol como o idioma do país em que estão), enquanto que todas ou certas informações sobre proteção de dados estão disponíveis apenas em inglês.

Variação B: Cada vez que os usuários chamam certas páginas, como a página de ajuda, estas mudam automaticamente para o idioma do país em que os usuários estão, mesmo

76. A Variação A ilustra o caso em que nenhuma informação está disponível em um idioma aparentemente dominado pelo sujeito dos dados. Isto significa que eles não podem ler as informações e, por extensão, não podem entender como seus dados pessoais são processados. A informação não pode ser considerada inteligível como exigido no Artigo 12 (1) da GDPR. Devido à falta de informações de proteção de dados no idioma compreensível, as informações exigidas pelo Artigo 13 respectivamente 14 GDPR não podem ser consideradas como tendo sido fornecidas aos titulares dos dados.

77. A Variação B descreve um caso em que as páginas de informações sobre proteção de dados são, por padrão, apresentadas no idioma do país de residência do usuário, apesar de sua clara escolha de idioma. Isto significa que os usuários têm que redefinir sua preferência de idioma cada vez que acessam uma página de informações sobre proteção de dados. Isto pode ser considerado como uma prática desleal para com os sujeitos dos dados e pode contribuir para uma violação do princípio de justiça do Artigo 5 (1) (a) GDPR.

ii. Padrões baseados em interfaces

78. Em alguns casos, os provedores de mídia social fazem uso de práticas específicas para apresentar suas configurações de proteção de dados. Durante o processo de inscrição, os usuários recebem muitas informações e diferentes configurações relacionadas à proteção de dados. Para garantir que os usuários possam encontrar seu caminho até essas configurações e fazer alterações

[42] Ver Diretrizes sobre transparência, para. 12, incluindo os "Exemplos de más práticas", e para. 13.
[43] Ver Diretrizes sobre transparência, para. 13 e nota de rodapé 15.

em qualquer ponto ao utilizar a plataforma, as configurações devem ser facilmente acessíveis e associadas a informações relevantes para que os usuários tomem uma decisão informada. O elemento "facilmente acessível" significa que os sujeitos dos dados não devem ter que buscar as informações. Com relação às políticas de privacidade, o Grupo de Trabalho do Artigo 29 já declarou que um posicionamento ou esquemas de cores que tornam um texto ou link menos perceptível, ou difícil de encontrar em uma página web, não são considerados de fácil acesso.[44]

Sobrecarga - Labirinto de Privacidade (Anexo I lista de verificação 4.1.2)

79. De acordo com as Diretrizes sobre Transparência, o aviso sobre privacidade deve ser facilmente acessível, ou seja, através de um clique nos websites.[45] O uso do método de abordagem em camadas pode ajudar a apresentar a nota de privacidade mais claramente no sentido do Artigo 12 (1) GDPR.[46] Entretanto, isto não deve resultar em tornar o exercício de funções ou direitos importantes desnecessariamente difícil, fornecendo uma política de privacidade complexa que consiste em inúmeras camadas que resultariam no ***labirinto de privacidade*** enganoso padrão de design. Este padrão corresponde a um controle de informações ou de proteção de dados sendo particularmente difícil de encontrar, pois os usuários têm que navegar por muitas páginas sem ter uma visão abrangente e exaustiva disponível. Isto provavelmente faz com que os usuários ignorem as informações/ajustes relevantes ou desistam de procurá-las. A disposição em camadas destina-se a facilitar a legibilidade e dar informações sobre como exercer os direitos do sujeito dos dados, e não a torná-los mais difíceis. É central para garantir que os usuários possam facilmente seguir as explicações.

80. Nesse sentido, o melhor para os usuários não é uma abordagem de tamanho único e depende de muitos critérios, tais como o tipo de usuários na plataforma ou o tipo geral de projeto da aplicação. Sempre que possível, o teste da abordagem em camadas implementada com os usuários para obter seu feedback deve ser realizado para avaliar sua eficácia. Por esta razão, nenhum número concreto pode ser quantificado para o número máximo de camadas de informação permitidas. Portanto, deve ser sempre determinado caso a caso se são usadas demasiadas camadas e, portanto, se ocorrem padrões de projeto enganosos. Entretanto, quanto maior o número, mais se pode supor que os usuários serão desencorajados ou enganados. Um número elevado de camadas só será apropriado para casos individuais especiais, nos quais não é fácil fornecer as informações complexas de forma abrangente. Ao mesmo tempo, a abordagem em camadas não pode ser mal utilizada para esconder informações em camadas mais profundas ou adicionando camadas desnecessárias.

81. Entretanto, isto deve ser avaliado de forma diferente quando se trata do exercício dos direitos dos usuários. A GDPR exige que o exercício destes direitos seja sempre concedido. Esta estrutura determina a apresentação de informações sobre funções relacionadas e o exercício dos direitos. Quando os usuários querem exercer seus direitos, o número de etapas deve ser o mais baixo possível. Como resultado, os usuários devem chegar à função que lhes permite exercer seus direitos da forma mais direta possível. Na maioria dos casos, ter que navegar por um alto número de camadas de informação antes que os usuários possam realmente exercer seus direitos através de funções poderia desencorajá-los de exercer esses direitos. Se um alto número de passos for implementado, o provedor de mídia social deve ser capaz de demonstrar o benefício que isso tem para os usuários como sujeitos de dados sob o GDPR. Além da explicação dos direitos dos sujeitos dos dados no aviso sobre privacidade, conforme exigido pelo Artigo 13 (2) (b), (c) e (d) da GDPR, o exercício dos direitos também deve ser acessível independentemente destas informações. Por exemplo, os usuários devem poder exercer os direitos dos sujeitos dos dados também através do menu da plataforma.

[44] Diretrizes sobre transparência, para. 11.
[45] Ver Diretrizes sobre transparência, exemplo no parágrafo. 11.
[46] Para obter detalhes sobre a abordagem em camadas em um ambiente digital, veja Diretrizes sobre transparência, para. 35-37.

Exemplo 17: Em sua plataforma, o provedor de mídia social disponibiliza um documento chamado "*conselhos úteis*" que também contém informações importantes sobre o exercício dos direitos do sujeito dos dados. Entretanto, a política de privacidade não contém nenhum link ou outra dica para este documento. Ao invés disso, ela menciona que mais detalhes estão disponíveis na seção de perguntas e respostas do site. Os usuários que esperam informações sobre seus direitos na política de privacidade não encontrarão, portanto, estas

82. Este exemplo mostra claramente um padrão de ***Labirinto de Privacidade*** que torna o acesso a mais informações sobre os direitos do sujeito dos dados, e em particular sobre como exercê-los, mais difícil de encontrar do que deveria, ao contrário do Artigo 12 (2) GDPR. Além disso, se a política de privacidade estiver incompleta, isso também infringe o Artigo 13 (2) (b), (c) e (d), respectivamente o Artigo 14 (2) (c), (d) e (e) GDPR. De fato, enquanto informações mais detalhadas ou o meio direto de exercer os direitos poderiam estar a um clique de distância de onde são mencionados na política de privacidade, os usuários no exemplo terão que navegar até as Perguntas e Respostas e pesquisá-las para encontrar o documento de "*conselhos úteis".*

83. É importante notar que efeitos ainda mais fortes do que os causados por demasiadas camadas[47] pode ocorrer quando não apenas vários dispositivos, mas também vários aplicativos fornecidos pela mesma plataforma de mídia social, como aplicativos especiais de mensageiros, são utilizados. Os usuários que utilizam esse tipo de aplicativo secundário enfrentariam maiores obstáculos e esforços se tivessem que chamar a versão do navegador ou o aplicativo principal para obter informações relacionadas à proteção de dados. Em tal situação, que não é apenas uma aplicação cruzada, mas uma aplicação cruzada, as informações relevantes devem ser sempre diretamente acessíveis, não importa como os usuários utilizam a plataforma.

Obstrução - Ponto morto (Anexo I lista de verificação 4.4.1)

84. As violações das exigências legais também podem ocorrer quando as informações sobre proteção de dados exigidas pela GDPR são disponibilizadas através de outras ações, tais como clicar em um link ou botão. Em particular, a navegação mal direcionada ou o design inconsistente da interface que leva a características ineficazes não podem ser classificados como justos sob o Artigo 5 (1) (a) GDPR, pois os usuários são enganados quando tentam chegar a alguma informação ou definem suas preferências de proteção de dados. Portanto, devem ser evitados os ***becos sem saída*** onde os usuários são deixados sozinhos sem funções para perseguir seus direitos e violar diretamente o artigo 12 (2) da GDPR, que declara que o controlador tem que facilitar o exercício dos direitos.

Exemplo 18: Em sua política de privacidade, um provedor de mídia social oferece muitos hyperlinks para páginas com mais informações sobre tópicos específicos. No entanto, há várias partes na política de privacidade contendo apenas declarações gerais de que é possível acessar mais informações, sem dizer onde ou como.

85. A política de privacidade é geralmente vista como o documento que centraliza todas as informações relativas às questões de proteção de dados de acordo com as obrigações estabelecidas nos artigos 12, 13 e 14 da GDPR. Portanto, é necessário também assegurar o redirecionamento para todos os lugares relevantes na plataforma de mídia social para que os usuários possam controlar seus dados ou exercer seus direitos. No exemplo 18 acima, isto só é implementado parcialmente, pois são fornecidos links para informações adicionais para alguns elementos, mas não para outros. Para estes, o padrão de ***Dead end*** pode levar a uma violação do Artigo 12 (1) GDPR, tornando algumas informações de proteção de dados difíceis de acessar, ou do Artigo 12 (2) GDPR, por não facilitar o exercício dos direitos.

d. **As melhores práticas**

[47] Ver acima, para. 81 e 82.

Navegação pegajosa: Ao consultar uma página relacionada à proteção de dados, o índice pode ser exibido constantemente na tela permitindo aos usuários sempre se situar na página e navegar rapidamente no conteúdo graças aos links de ancoragem.

Voltar ao início: Incluir um botão de retorno ao topo na parte inferior da página ou como um elemento pegajoso na parte inferior da janela para facilitar a navegação dos usuários em uma página.

Atalhos: ver caso de uso 1 para definição (p. 22). (por exemplo, *na política de privacidade, fornecer para cada link de informação de proteção de dados que redireciona diretamente para as páginas de proteção de dados relacionadas na plataforma de mídia social*).

Informações de contato: ver caso de uso 1 para definição (p. 22).

Chegar à autoridade supervisora: ver caso de uso 1 para definição (p. 22).

Visão geral da política de privacidade: ver caso de uso 1 para definição (p.22).

Mudança de mancha e comparação: ver caso de uso 1 para definição (p. 22).

Palavras coerentes: ver caso de uso 1 para definição (p.

22). **Fornecer definições**: ver caso de uso 1 para definição

(p. 22). **Uso de exemplos: ver caso de** uso 1 para definição

Use o caso 2b: Fornecimento de informações sobre o controle conjunto ao sujeito dos dados, Artigo 26 (2) GDPR

a. Descrição do contexto e disposições legais relevantes

86. A segunda frase do Artigo 26 (2) GDPR prevê disposições adicionais de transparência no caso específico de controladoria conjunta.[48] Estas asseguram que a essência do acordo de controle conjunto seja colocada à disposição dos sujeitos dos dados.[49] Em suas Diretrizes 07/2020 sobre os conceitos de controlador e processador na GDPR, a EDPB recomenda que a essência abranja pelo menos todos os elementos das informações referidas nos artigos 13 e 14 da GDPR que já devem estar acessíveis aos sujeitos dos dados, e especificar para cada elemento qual controlador conjunto é responsável por garantir o cumprimento do mesmo.[50] A essência do acordo também deve indicar o ponto de contato, se designado. Cabe aos co-controladores decidir a maneira mais eficaz de tornar a essência do arranjo disponível para os sujeitos dos dados.[51]

b. Padrões de design enganosos

Exemplo 19: Com relação aos padrões de design enganosos, o desafio para os controladores desta constelação é integrar estas informações no sistema on-line de tal forma que possam ser facilmente percebidas e não percam sua clareza e compreensibilidade, ainda que O artigo 12 (1) frase 1 GDPR não se refere diretamente ao artigo 26 (2) frase 2 GDPR.

[48] Para a definição de controladoria conjunta, veja o Artigo 4 (7) em conjunto com o Artigo 26 (1) frase 1 GDPR, assim como as Diretrizes 07/2020 da EDPB sobre os conceitos de controlador e processador na GDPR, adotadas em 7 de julho de 2021, versão 2.1, para. 46-49, disponível em https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[49] Ver Diretrizes EDPB 07/2020 sobre controlador e processador, para. 179.

[50] Ver Diretrizes EDPB 07/2020 sobre controlador e processador, para. 180, também para a próxima frase.

[51] Diretrizes EDPB 07/2020 sobre controlador e processador, para. 181.

Entretanto, devido aos princípios de proteção de dados de justiça, transparência e responsabilidade nos termos do Artigo 5 (1) (a) e (2) GDPR, exigências comparáveis derivam também do caso de controle conjunto. Quando os controladores conjuntos fornecem informações sobre a essência do acordo em uma notificação de privacidade, isto também precisa ser feito de forma clara e transparente. Portanto, o processamento não pode mais ser avaliado como justo se a informação sobre ele for dificultada porque os links não são fornecidos ou a informação está espalhada por várias áreas de informação. O padrão de design enganoso ***Privacy Maze***[52] poderia ser ainda mais confuso do que, geralmente, em um aviso de privacidade, pois os usuários podem esperar que as informações de acordo com a frase 2 do Artigo 26 (2) do GDPR sejam fornecidas em uma única peça. Um provedor de mídia social sempre se refere a *"dados de criação"* dentro da política de privacidade e não usa o termo dados pessoais. Somente na página 90, o aviso de privacidade em camadas contém a explicação de que *"dados de criação podem incluir dados pessoais dos usuários"*. A essência do acordo de co-controle fornecido aos sujeitos dos dados também usa o termo "dados de criação", sem explicação. O outro controlador conjunto (B) tem uma definição de dados pessoais em sua própria política de privacidade. Entretanto, em sua seção de política de privacidade sobre controle conjunto com o provedor de mídia social, B fornece apenas

87. As explicações sob o artigo 26 (2) frase 2 GDPR são mais difíceis de conceber quando não são mais coerentes. Este efeito de incoerência é ampliado quando as plataformas de mídia social utilizam terminologia autocriada que os usuários normalmente não associam ao processamento de dados pessoais, como mostrado no exemplo 19 acima. No exemplo, ambos os controladores conjuntos infringem a frase (2) do Artigo 26 (2) GDPR, bem como o Artigo 5 (1) (a) GDPR porque as informações fornecidas sobre o controle conjunto não são claras e, portanto, não são transparentes para os sujeitos dos dados.

Caso de uso 2c: Comunicação de uma violação de dados pessoais ao titular dos dados

a. Descrição do contexto e disposições legais relevantes

88. Para ser capaz de identificar e tratar uma violação de dados, um controlador tem que ser capaz de reconhecer uma.[53] De acordo com o Artigo 4 (12) da GDPR, "violação de dados pessoais" significa "uma violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação ou acesso não autorizado a dados pessoais transmitidos, armazenados ou de outra forma processados". Quando se trata de controladores de mídia social, as violações de dados podem acontecer de várias maneiras. Por exemplo, se um atacante conseguir acessar dados pessoais e mensagens de bate-papo dos usuários. Alternativamente, devido a uma falha de programação, um aplicativo poderia acessar dados pessoais fora do escopo das permissões concedidas pelos usuários. Outro exemplo seria que os usuários compartilham imagens sob o cenário "compartilhar com meus melhores amigos", mas suas imagens são disponibilizadas a um maior número de pessoas. Como último exemplo, um bug poderia permitir que uma plataforma de mídia social baseada em vídeo em tempo real compartilhasse mais streaming de conteúdo, apesar de os usuários terem pressionado anteriormente um botão para interromper a gravação.

89. Se ocorrer uma violação de dados pessoais, o controlador deverá, em qualquer caso, notificar a autoridade de supervisão competente de acordo com o Artigo 33 GDPR, a menos que a violação de dados pessoais seja improvável de resultar em risco aos direitos e liberdades de pessoas físicas. Se uma violação de dados for susceptível de resultar em alto risco para os direitos

[52] Veja acima, use o caso 2a, exemplo 17 nestas Diretrizes.
[53] Veja também as Diretrizes EDPB 01/2021 sobre Exemplos de Notificação de Violação de Dados, adotadas em 14 de dezembro de 2021, Versão 2.0, para. 4, disponível em https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

e liberdades das pessoas físicas, o responsável pelo tratamento também comunicará, em geral, tal violação às pessoas em questão, de acordo com o Artigo 34 (1) e (2) GDPR. Neste caso, o responsável pelo tratamento deve informar as pessoas em questão sem demora injustificada. Esta informação deve descrever em linguagem clara e clara a natureza da violação dos dados pessoais, como também se aplica o Artigo 12 da GDPR. Além disso, estas informações devem conter pelo menos informações e medidas tais como (ver também artigo 33 (3) (b) a (d) em conjunto com o artigo 34 (2) GDPR):

- o nome e detalhes de contato do encarregado da proteção de dados (DPO), se aplicável, ou outro ponto de contato onde mais informações podem ser obtidas;
- uma descrição das prováveis conseqüências da violação de dados pessoais; e
- uma descrição das medidas tomadas ou propostas a serem tomadas pelo controlador para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.[54]

90. Tais comunicações de violação de dados sob o Artigo 34 GDPR também podem conter padrões de design enganosos. Por exemplo, se o respectivo controlador fornecer todas as informações necessárias aos sujeitos dos dados para informá-los sobre o escopo da violação de dados, mas também lhes fornecer informações não específicas e irrelevantes e as implicações e medidas de precaução que o controlador tenha tomado ou sugerido tomar. Esta informação parcialmente irrelevante pode ser enganosa e os usuários afetados pela violação podem não compreender totalmente as implicações da violação ou subestimar os efeitos (potenciais).

b. Padrões de design enganosos

91. Para delinear alguns exemplos negativos, as más práticas de notificações de violação de dados, infringindo o Artigo 34 GDPR em conjunto com o Artigo 12 GDPR, poderiam ocorrer da seguinte forma:

i. Padrões baseados no conteúdo

Esquerda no escuro - Informações conflitantes (Anexo I lista de verificação 4.6.2)

Exemplo 20:

- O controlador se refere apenas a ações de terceiros, que a violação dos dados foi por um terceiro (por exemplo, um processador) e que, portanto, nenhuma violação de segurança ocorreu. O controlador

- O controlador declara a gravidade da violação dos dados em relação a si mesmo processador, e não em relação à pessoa em questão.

Esquerda na escuridão - texto ou informações ambíguas (Anexo I lista de verificação 4.6.3)

92. Quando se trata da linguagem de comunicação da violação ao envolvido, é crucial que os controladores tenham em mente que a maioria dos destinatários não estará acostumada a linguagem específica, talvez técnica ou legal relacionada à proteção de dados.

[54] Artigo 29 Diretrizes do Grupo de Trabalho sobre notificação de violação de dados pessoais, endossadas pela EDPB, p. 20 https://ec.europa.eu/newsroom/article29/items/612052/en.

> **Exemplo 21:** Através de uma violação de dados em uma plataforma de mídia social, vários conjuntos de dados de saúde foram acidentalmente acessíveis a usuários não autorizados. O provedor de mídia social apenas informa aos usuários que "*categorias especiais de*

93. Isto constitui uma ***formulação ambígua***, pois os usuários médios não entendem o termo "*categorias especiais de dados pessoais"* e, portanto, não sabem que seus dados de saúde foram vazados. Isto se deve ao fato de que "especial" tem um significado muito diferente na linguagem geral do que "especial" no uso restrito da linguagem relacionada ao GDPR. Os usuários médios não sabem que, nos termos do Artigo 9 (1) GDPR, *"categorias especiais de dados pessoais"* referem-se a dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, ou dados genéticos, dados biométricos com a finalidade de identificar de forma única uma pessoa física, ou dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física. Assim, a designação *"categorias especiais de dados pessoais"* constitui um padrão de design enganoso neste cenário, pois engana os usuários, pois não é acompanhada de explicações adicionais. Este é um exemplo de uma situação em que um controlador tenta informar as pessoas em questão sobre a violação, mas não cumpre plenamente sua obrigação de comunicar a violação de dados de acordo com o Artigo 34 GDPR porque a gravidade do incidente será subestimada pelo leitor médio. A breve informação no exemplo também não é inteligível, como exigido pelo Artigo 34 em conjunto com a frase 1 do Artigo 12 GDPR.

94. Outro exemplo de ***formulação ambígua*** é o seguinte:

> **Exemplo 22:** O controlador só fornece detalhes vagos ao identificar as categorias de dados pessoais afetados, por exemplo, o controlador se refere a documentos apresentados pelos usuários sem especificar que categorias de dados pessoais esses documentos incluem e quão sensíveis eles eram.

95. É importante observar que este padrão de projeto enganoso pode ocorrer em todas as partes da notificação de violação de dados. Enquanto os dois exemplos mencionados acima se referem a uma formulação pouco clara sobre as categorias de dados afetados, o exemplo seguinte mostra que a categoria dos sujeitos dos dados afetados poderia ser igualmente pouco clara:

> **Exemplo 23:** Ao comunicar a violação, o controlador não especifica suficientemente a categoria dos indivíduos afetados, por exemplo, o controlador só menciona que os indivíduos em questão eram estudantes, mas não especifica se os indivíduos são menores ou grupos de indivíduos vulneráveis.

96. Finalmente, a gravidade do incidente também pode ser subestimada quando ***informações ambíguas*** são dadas de forma semelhante ao exemplo abaixo:

> **Exemplo 24:** Um controlador declara que os dados pessoais foram tornados públicos através de outras fontes quando notifica a violação à Autoridade Supervisora e ao titular dos dados. Portanto, a pessoa em questão considera que não houve violação de segurança.

ii. Padrões baseados em interfaces

97. Exemplos negativos de uma notificação de violação de dados, contrariamente ao Artigo 34 GDPR em conjunto com o Artigo 12 GDPR, também podem constituir padrões de projeto enganosos baseados em interface, como mostrado a seguir:

Skipping - Veja ali (Anexo I lista de verificação 4.2.2)

Exemplo 25:

- O controlador informa através de textos que contêm muitas informações não relevantes e omitem os detalhes relevantes.
- Em violações de segurança que afetam as credenciais de acesso e outros tipos de dados, o controlador declara que os dados são criptografados ou hashed, enquanto que este é

98. Neste caso, mesmo que os detalhes relevantes estejam no relatório, é provável que os sujeitos dos dados sejam desviados dele por uma sobrecarga de informações irrelevantes.

c. As melhores práticas

Notificações: As notificações podem ser usadas para conscientizar os usuários sobre aspectos, mudanças ou riscos relacionados ao processamento de dados pessoais (por exemplo, *quando uma violação de dados ocorreu*). Estas notificações podem ser implementadas de várias maneiras, tais como através de mensagens na caixa de entrada, janelas pop-in, banners fixos no topo da página da web, etc.

Explicando as conseqüências: Quando os usuários querem ativar ou desativar um controle de proteção de dados, ou dar ou retirar seu consentimento, informá-los de forma neutra sobre as conseqüências de tal ação.

Atalhos: ver caso de uso 1 para definição (p.22) (por *exemplo, fornecer aos usuários um link para redefinir sua senha*).

Palavras coerentes: ver caso de uso 1 para definição (p.22).

3.3 Ficar protegido nas mídias sociais

Caso de uso 3a: Gerenciamento do consentimento enquanto se utiliza uma plataforma de mídia social

a. Descrição do contexto e disposições legais relevantes

99. Os usuários da plataforma de mídia social precisam fornecer seu respectivo consentimento durante diferentes partes das atividades de processamento de dados, por exemplo, antes de receberem publicidade personalizada. Como já delineado nas Diretrizes da EDPB sobre o direcionamento de usuários de mídia social, o consentimento só pode ser uma base legal apropriada se for oferecido ao sujeito dos dados controle e escolha genuína.55 Além disso, de acordo com o Artigo 4 (11) da GDPR, o consentimento deve ser específico, informado e inequívoco.56 É importante salientar que os requisitos para consentimento válido sob a GDPR não constituem uma obrigação adicional, mas são condições prévias para o processamento lícito dos dados pessoais dos usuários. Além disso, quando se trata de marketing on-line ou métodos de rastreamento on-line, a Diretiva 2002/58/CE (Diretiva e-Privacy) é aplicável. Entretanto, os pré-requisitos para o consentimento válido sob a Diretiva de Privacidade Eletrônica são idênticos às disposições relacionadas ao consentimento na GDPR.57

[55] Diretrizes 08/2020 sobre o direcionamento dos usuários das mídias sociais, para 51.
[56] Ver também os parágrafos 25-29 acima.
[57] Ver artigo 2(f) da Diretiva 2002/58/CE, bem como EDPB, Parecer 5/2019 sobre a interação entre a Diretiva ePrivacy e a GDPR, em particular no que diz respeito à competência, tarefas e poderes das autoridades de

proteção de dados, adotado em 12 de março de 2019, para 14, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board- art-64/opinion-52019-interplay-between-eprivacy_en.

100. Dado o princípio de responsabilidade estabelecido no Artigo 5 (2) GDPR, bem como a necessidade de o responsável pelo controle poder demonstrar que as pessoas em questão consentiram no tratamento de seus dados pessoais nos termos do Artigo 7 (1) GDPR, é crucial que o fornecedor da mídia social possa provar ter o consentimento dos usuários devidamente coletado. Esta condição pode se tornar um desafio para provar, por exemplo, se os usuários devem dar seu consentimento aceitando cookies. Além disso, os sujeitos dos dados podem nem sempre estar cientes de que estão dando consentimento enquanto clicam rapidamente em um botão destacado ou em opções pré-definidas. Entretanto, como sublinha o Artigo 7 (1) da GDPR, o ônus da prova de que os usuários deram livremente o consentimento depende do controlador.

b. Padrões de design enganosos

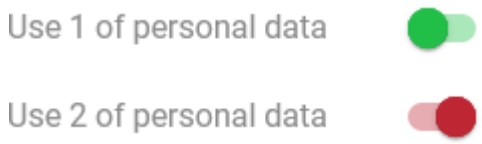
i. Padrões baseados no conteúdo

101. Além dos padrões baseados no conteúdo já explicados anteriormente que poderiam se aplicar às informações relacionadas a um pedido de consentimento,[58] mais dois padrões de design enganosos baseados em conteúdo podem ser encontrados em relação ao consentimento.

Informações conflitantes - Esquerda no escuro (Anexo I lista de verificação 4.6.2)

Exemplo 26: A interface usa um interruptor para permitir que os usuários dêem ou retirem o consentimento.

Entretanto, a forma como a chave múltipla é projetada não deixa claro em que posição ela está e se os usuários deram ou não o consentimento. De fato, a posição da chave múltipla não corresponde à cor. Se a chave múltipla estiver do lado direito, que normalmente está associada à ativação do recurso ("ligar"), a cor da chave é vermelha, o que normalmente significa que um recurso está desligado. Por outro lado, quando o interruptor está no lado esquerdo, o que geralmente significa que o recurso está desligado, a cor de fundo do alternador é verde, que normalmente está associada a uma opção ativa.



102. Fornecer ***informações conflitantes*** ao coletar consentimento torna as informações pouco claras e ininteligíveis. O exemplo acima ilustra um caso em que a informação visual é equívoca. De fato, confrontados com tais alternâncias, os usuários ficarão inseguros se deram ou não seu consentimento. Quando os significantes visuais são misturados de tal forma ou apresentados em outras cores que parecem contraditórias com o cenário real - exemplo 26 contendo apenas uma ilustração de comutadores confusos -, o consentimento não pode ser considerado como dado de forma inequívoca, sob o Artigo 7 (2) GDPR, em conjunto com o Artigo 4 (11) GDPR. ***Informações conflitantes*** também podem ser dadas por meios textuais, como mostrado abaixo.

[58] Ver caso de uso 1, para. 32-49, ou números de exemplo UC1 listados no Anexo.

Exemplo 27: O provedor de mídia social fornece informações contraditórias aos usuários: Embora as informações primeiro afirmem que os contatos não são importados sem consentimento, uma janela pop-up de informações simultaneamente explica como os contatos serão

Obstrução - Ação enganosa (Anexo I lista de verificação 4.4.3)

103. Além de fornecer ***informações conflitantes***, os controladores podem implementar informações que induzem os usuários ao erro, não correspondendo às suas expectativas. A ***ação enganosa*** é quando uma discrepância entre informações e ações disponíveis aos usuários os impele a fazer algo que eles não pretendem fazer. A diferença entre o que os usuários esperam e o que eles recebem provavelmente os desencoraja de ir mais longe.

Exemplo 28: Os usuários navegam no feed de suas mídias sociais. Ao fazer isso, são mostrados anúncios. Intrigados por um anúncio e curiosos sobre os motivos que lhes são mostrados, eles clicam em um sinal "?" disponível no canto inferior direito do anúncio. Ela abre uma janela pop-in que explica por que os usuários vêem este anúncio em particular e lista os critérios de segmentação. Ela também informa aos usuários que eles podem retirar seu consentimento ao anúncio direcionado e fornece um link para fazer isso. Quando os usuários clicam neste link, são redirecionados para um site totalmente diferente, dando

104. O caso acima exemplifica o conteúdo que não responde às expectativas dos usuários. De fato, quando os usuários clicam no link, eles esperam ser redirecionados para uma página que lhes permita retirar diretamente seu consentimento. A página que lhes é fornecida não lhes permite fazê-lo e não indica a forma específica de retirar seu consentimento na plataforma de mídia social. Esta lacuna entre o que os usuários devem encontrar e o que eles realmente encontram é susceptível de confundi-los e deixá-los inseguros sobre como proceder. Na pior das hipóteses, eles poderiam acreditar que não podem retirar seu consentimento. Tal ***ação enganosa*** não pode ser considerada transparente como exigido no artigo 12 (1) da GDPR. Além disso, comparando a retirada com a forma como o consentimento é coletado, esta prática poderia infringir o Artigo 7 (3) GDPR se a retirada do consentimento se revelasse mais difícil do que dar o consentimento.

105. Quando os provedores de mídia social informam aos usuários que uma ação de sua parte pode ter uma certa conseqüência e a ação realmente leva a um resultado diferente, isto constitui uma ***ação enganosa***, como mostrado no próximo exemplo.

Exemplo 29: Na parte da conta da mídia social onde os usuários podem compartilhar pensamentos, fotos, etc., é pedido que eles confirmem que gostariam de compartilhar este conteúdo uma vez que o tenham digitado ou carregado. Os usuários podem escolher entre um botão que diz "*Sim, por favor*" e outro que diz "*Não, obrigado*". Entretanto, uma vez que os usuários decidam não compartilhar o conteúdo com outros, clicando no segundo botão, o conteúdo é publicado em sua conta de mídia social.

106. Como no exemplo anterior, estas informações não são transparentes e afastam a escolha dos usuários. Mesmo que os usuários possam perceber rapidamente a publicação e apagá-la novamente, os dados foram processados apesar de sua recusa, e disponibilizados a outros. Um exemplo pior pode ser encontrado quando o processamento não é perceptível para os usuários ou apenas com dificuldade ou conhecimento de tecnologia da informação, pois ocorre no fundo da plataforma de mídia social.

ii. Padrões baseados em interfaces

107. Além dos dois padrões de design enganosos acima, são principalmente os padrões baseados em interface que são relevantes neste caso de uso.

Skipping - Veja ali (Anexo I lista de verificação 4.2.2)

108. Quando uma ação ou informação relacionada à proteção de dados é colocada em concorrência com outro elemento relacionado ou não à proteção de dados, se os usuários escolherem esta outra opção, eles provavelmente esquecerão a outra, mesmo que fosse sua intenção principal. Este é um padrão que precisa ser avaliado caso a caso.

> **Exemplo 30:** Um banner de biscoitos na plataforma de mídia social diz: "Para biscoitos deliciosos, você só precisa de manteiga, açúcar e farinha". Confira nossa receita favorita aqui [link]. Nós também usamos cookies. Leia mais em nossa política de biscoitos [link]",

109. O humor não deve ser usado para deturpar os riscos potenciais e invalidar as informações reais. Neste exemplo, os usuários podem ser tentados a apenas clicar no primeiro link, ler a receita do cookie e depois clicar no botão *"ok".* Além de não fornecer aos usuários um meio de não consentir, este exemplo ilustra um caso em que o consentimento pode não ser devidamente informado. De fato, ao clicar no botão *"ok"*, os usuários podem pensar que simplesmente descartam uma mensagem engraçada sobre cookies como um lanche assado e não consideram o significado técnico do termo *"cookies"*. Este caso não constituiria consentimento informado no sentido do artigo 7 (2) GDPR em conjunto com o artigo 4 (11) GDPR.

110. O artigo 7 (2) da GDPR estabelece ainda que um pedido de consentimento deve ser claramente distinguível de outros assuntos. Portanto, é necessário que as informações sobre proteção de dados não sejam ofuscadas por outros contextos. Neste exemplo, o jogo de palavras baseado em homônimos "cookie" pode fazer com que o contexto da padaria supere o contexto da proteção de dados. Para que as informações sejam claramente distinguíveis, as informações relevantes para que os usuários dêem consentimento válido devem ser iniciais, não ***ocultas à vista***, e não misturadas com outros assuntos ou significados. Não deve haver confusão entre as informações de proteção de dados e outros tipos de conteúdo. Caso contrário, os usuários poderão se distrair das reais implicações do processamento de seus dados pessoais. Ao implementar estes pré-requisitos, os projetistas precisam ter alguma margem de manobra para tornar as informações atraentes.

Obstrução - Ponto morto (Anexo I lista de verificação 4.4.1)

111. Confusão ou distração não é o único efeito possível com padrões de design enganosos quando se trata de consentimento. Em particular, o padrão de ***Dead end*** pode interferir de várias maneiras com as condições de consentimento estabelecidas no Artigo 7 GDPR em conjunto com o Artigo 4 (11) GDPR.

> **Exemplo 31:** Os usuários querem gerenciar as permissões dadas à plataforma de mídia social com base no consentimento. Eles têm que encontrar uma página nas configurações relacionadas a essas ações específicas e desejam desativar o compartilhamento de seus dados pessoais para fins de pesquisa. Quando os usuários clicam na caixa para desmarcá-la, nada acontece no nível da interface e eles têm a impressão de que o consentimento não

112. Neste exemplo específico, o padrão de ***Dead end*** poderia infringir o Artigo 7 (3) da GDPR, pois os usuários parecem não poder retirar seu consentimento para o processamento de seus dados

pessoais para fins de pesquisa, pois o meio de fazê-lo aparentemente não está funcionando. Se a ação dos usuários não for devidamente registrada dentro do sistema, uma violação do Artigo 7 (3) GDPR pode ser observada. Se a escolha for realmente registrada

no sistema, o fato de a interface não refletir a ação dos usuários poderia ser considerado como não respeitando o princípio de justiça do Artigo 5 (1) (a) GDPR. Quando uma interface parece oferecer os meios para administrar adequadamente o consentimento, permitindo aos usuários dar o consentimento ou retirar um consentimento previamente dado, mas não produz qualquer efeito visual quando interagida, é enganosa para o usuário e cria confusão e até mesmo frustração para ele. Tal lacuna entre o estado em que o sistema se encontra e as informações transmitidas pela interface deve ser evitada, pois geralmente pode dificultar o controle de seus dados pessoais pelos usuários.

113. Muitas atividades de processamento envolvem várias partes, ou seja, outro controlador (conjunto) ou outro processador que esteja envolvido além do controlador ou processador com o qual a pessoa interessada está em contato direto.

> **Exemplo 32:** Um provedor de mídia social trabalha com terceiros para o processamento dos dados pessoais de seus usuários. Em sua política de privacidade, ele fornece a lista desses terceiros sem fornecer um link para cada uma de suas políticas de privacidade, simplesmente dizendo aos usuários para visitarem os sites de terceiros a fim de obterem informações sobre como essas entidades processam os dados e para exercerem seus

114. Este exemplo do padrão de ***Dead end*** mostra como o acesso às informações sobre o respectivo processamento é dificultado para os usuários. Dado que é provável que eles não recebam todas as informações relevantes sobre o processamento, pode-se considerar que tal prática infringe as exigências do Artigo 12 (1) GDPR de informações facilmente acessíveis. Se tal prática for usada em informações fornecidas para coletar consentimento, ela pode infringir as exigências do consentimento livre e esclarecido, conforme estabelecido no Artigo 7 (2) em conjunto com o Artigo 4 (11) GDPR, pois as informações seriam muito difíceis de serem alcançadas, fazendo com que os sujeitos dos dados não tenham pleno conhecimento das conseqüências de sua escolha.

Obstrução - Mais longa do que o necessário (Anexo I lista de verificação 4.4.2)

115. O artigo 7 (3) da GDPR estabelece que a retirada do consentimento deve ser tão fácil quanto dar o consentimento. As Diretrizes 05/2020 sobre consentimento nos termos do Regulamento 2016/679 aprofundam o assunto, afirmando que o consentimento deve ser dado e retirado através do mesmo meio. Isto implica utilizar a mesma interface, mas também implica que os mecanismos para retirar o consentimento devem ser facilmente acessíveis, por exemplo, através de um link ou um ícone disponível a qualquer momento enquanto se utiliza a plataforma de mídia social.

> **Exemplo 33:** Um fornecedor de mídia social não fornece uma opção direta de não participação no processamento de um anúncio direcionado, mesmo que o

116. O tempo necessário ou o número de cliques necessários para retirar o consentimento de alguém pode ser usado para avaliar se é efetivamente fácil de conseguir. A implementação do padrão de projeto enganoso ***Mais do que o necessário*** dentro da jornada do usuário para retirar seu consentimento, como mostrado no exemplo 33, vai contra estes princípios, violando assim o Artigo 7 (3) GDPR.

Sobrecarga - ***Labirinto de Privacidade (Anexo lista de verificação I 4.1.2)***

117. Conforme destacado nas Diretrizes 05/2020 sobre consentimento, informações sobre o processamento baseado no consentimento devem ser fornecidas aos sujeitos dos dados a fim de que eles possam tomar uma decisão informada.[59] Sem ele, o consentimento não pode ser considerado

como válido. As mesmas Diretrizes desenvolvem ainda mais as maneiras de fornecer

[59] Diretrizes 05/2020 sobre consentimento, para. 62-64.

informações, especificando que informações estratificadas podem ser usadas para isso. Entretanto, como mostrado no caso 2 a,[60] Os provedores de mídia social precisam ficar atentos para evitar o padrão de design enganoso ***do Labirinto de Privacidade*** ao fornecer informações relacionadas a um pedido de consentimento de forma estratificada. Se algumas informações se tornarem muito difíceis de encontrar, pois os sujeitos dos dados precisariam navegar por várias páginas ou documentos, o consentimento coletado ao fornecer tais informações não poderia ser considerado como informado, indo contra o Artigo 7 GDPR em conjunto com o Artigo 4 (11) GDPR. Por extensão, isto significaria que o consentimento é inválido e que o fornecedor da mídia social violaria o Artigo 6 da GDPR.

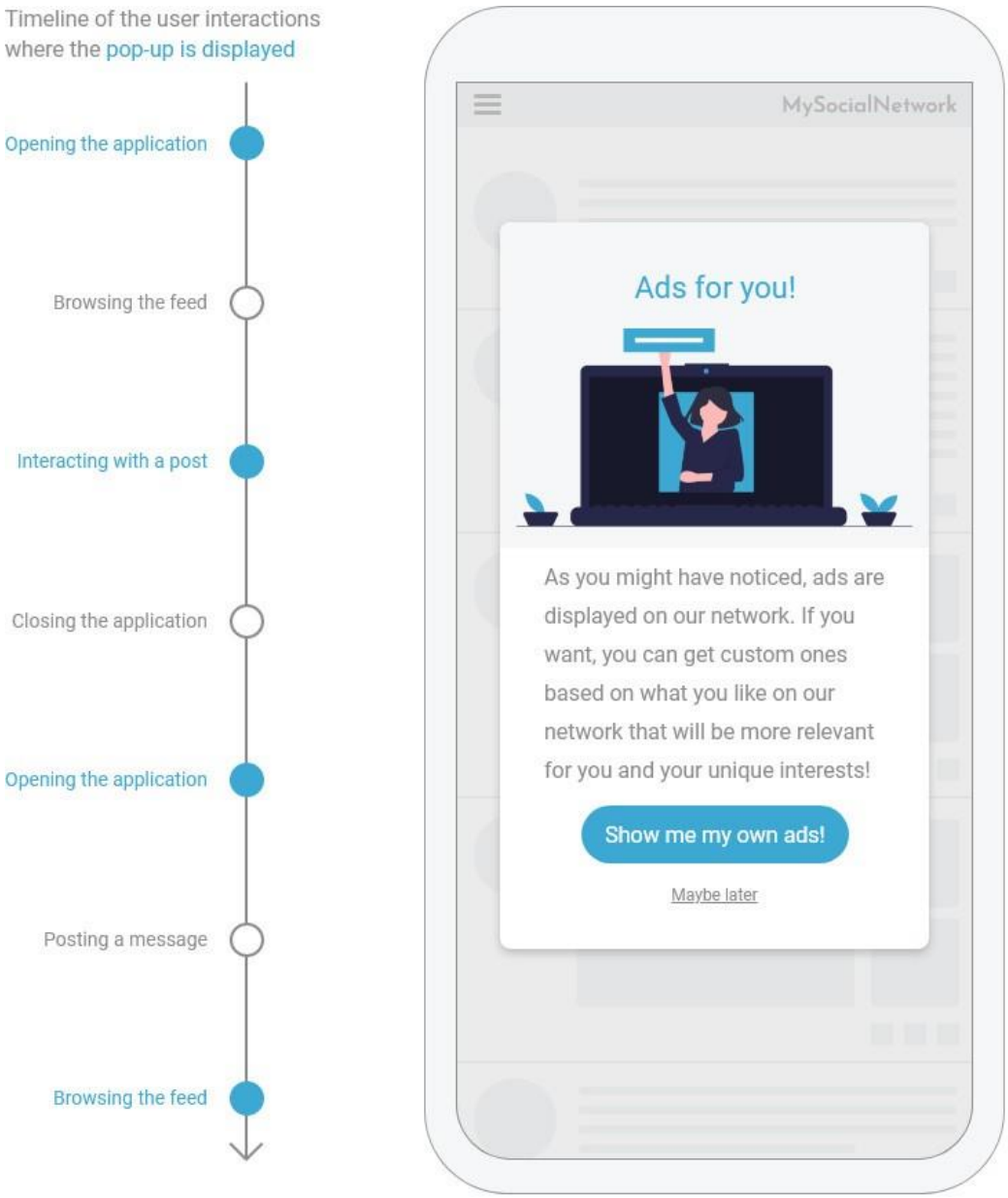
> **Exemplo 34:** Informações para retirar o consentimento estão disponíveis em um link acessível somente verificando cada seção de sua conta e informações associadas a anúncios exibidos no feed da mídia social.

118. Como o cenário descrito acima mostra, o padrão de design enganoso ***Privacy Maze*** também pode ser um problema uma vez que o consentimento é coletado, não respeitando a condição sob o Artigo 7 (3) frase 4 GDPR, que afirma que a retirada do consentimento deve ser tão fácil quanto dar o consentimento. Isto se deve especificamente ao fato de que o processo de retirada de consentimento inclui mais etapas do que a ação afirmativa de dar o consentimento. Como a informação fornecida também não é facilmente acessível ao interessado, já que está espalhada por diferentes partes da página, o princípio estabelecido no Artigo 12 (1) da GDPR é violado.

Sobrecarga - Alerta contínuo (Anexo I lista de verificação 4.1.1)

119. ***O Prompting contínuo***, quando usado em usuários que não consentiram o processamento de seus dados pessoais para um propósito específico, cria um obstáculo no uso regular das mídias sociais. Isto significa que os usuários não podem recusar o consentimento e, por extensão, retirá-lo, sem detrimento. Isto contraria a condição de consentimento livre e esclarecido, nos termos do artigo 7 em conjunto com o artigo 4 (11) da GDPR, que consentimento significa qualquer indicação livre e esclarecida da vontade das pessoas em causa, pela qual elas manifestam concordância com o tratamento dos dados pessoais a elas relativos. O considerando 42 frase 5 da GDPR afirma ainda que o consentimento não pode ser considerado dado livremente se os usuários não tiverem escolha genuína ou livre. Isto também é apoiado pelas Diretrizes da EDPB sobre consentimento, descrevendo que o consentimento não será válido se os sujeitos dos dados não tiverem escolha real ou se sentirem obrigados a consentir por qualquer elemento de pressão ou influência inadequada sobre eles, o que os impede de exercer seu livre arbítrio.[61] Como o ***Prompting Contínuo*** pode causar tal tipo de pressão, isto infringe o princípio do consentimento livre e esclarecido. Além disso, como é improvável que uma vez que os usuários tenham consentido, o provedor de mídia social ofereça regularmente (por exemplo, toda vez que eles retornarem à sua conta) a possibilidade de retirar o consentimento, este padrão enganoso pode infringir a frase 4 GDPR do Artigo 7 (3), estabelecendo que será tão fácil retirar quanto dar o consentimento ("efeito espelhado").

[60] Ver acima, para. 79-81.
[61] Diretrizes 05/2020 sobre consentimento, para. 13-14.



Exemplo 35: Neste exemplo, quando os usuários criam sua conta, eles são perguntados se aceitam que seus dados sejam processados para obter publicidade personalizada. Caso os usuários não consintam em se inscrever para este uso de seus dados, eles vêem regularmente - enquanto utilizam a rede social - a caixa de avisos ilustrada acima, perguntando se querem anúncios personalizados. Esta caixa os está bloqueando no uso da rede social. Sendo exibido regularmente, este ***incitamento contínuo*** provavelmente cansa os usuários a consentirem com a publicidade personalizada.
Além disso, nesta interface, o padrão ***Escondido à vista simples***[62] também é utilizada, pois a

120. Além disso, o controlador poderia infringir o princípio de justiça no sentido do Artigo 5 (1) (a) GDPR. Dado que, no exemplo acima, os usuários não consentiram por uma ação clara o processamento de seus dados pessoais para publicidade direcionada ao criar sua conta, a solicitação repetida

[62] Ver parágrafo acima. 49, ou abaixo, na parte 4.3.2 do Anexo.

constantemente colocando em questão uma recusa clara que eles fizeram é onerosa. Esta ação clara que os usuários tomaram durante o processo de registro é agora constantemente posta em questão. A degradação induzida da experiência do usuário aumenta significativamente a probabilidade de os usuários aceitarem o anúncio visado em algum momento, apenas para evitar serem questionados novamente toda vez que entrarem em sua conta e desejarem usar a plataforma de mídia social. Neste caso, não dar o consentimento tem um impacto direto na qualidade do serviço prestado aos usuários e condiciona a execução do contrato.

c. As melhores práticas

Consistência de dispositivos cruzados: Quando a plataforma de mídia social está disponível através de diferentes dispositivos (por exemplo, computador, smartphones, etc.), as configurações e informações relacionadas à proteção de dados devem estar localizadas nos mesmos espaços através das diferentes versões e devem ser acessíveis através da mesma viagem e elementos de interface (menu, ícones, etc.).

Mudança de mancha e comparação: ver caso de uso 1 para definição (p. 22)**.**

Palavras coerentes: ver caso de uso 1 para definição (p. 22).

Fornecer definições: ver caso de uso 1 para definição (p. 22).

Uso de exemplos: ver caso de uso 1 para definição (p. 22).

Navegação pegajosa: ver caso de uso 2a para definição (p.

28). **Voltar ao início**: ver caso de uso 2a para definição

(pág. 28).

Usar o caso 3b: Gerenciar as configurações de proteção de dados

a. Descrição do contexto

121. Após completar o processo de inscrição, e durante todo o ciclo de vida de sua conta de mídia social, os usuários devem ser capazes de ajustar suas configurações de proteção de dados.

122. Quer os usuários tenham conhecimento prévio da proteção de dados em geral e da GDPR em particular ou não, e se estão atentos aos dados pessoais que compartilham ou não e outros que desejam ver, todos têm o direito de serem informados sobre suas possibilidades de forma transparente enquanto utilizam uma mídia social.

123. Os usuários compartilham uma grande quantidade de dados pessoais em plataformas de mídia social. Eles são freqüentemente encorajados pelas plataformas de mídia social a continuar compartilhando mais regularmente. Embora os usuários possam querer compartilhar momentos de sua vida, participar de um debate sobre um assunto ou ampliar suas redes de contatos, seja por razões profissionais ou pessoais, eles também precisam receber as ferramentas para controlar quem pode ver quais partes de seus dados pessoais. Uma maneira de evitar multiplicar o número de passos necessários para mudar a configuração de uma pessoa seria projetar um painel de privacidade que permita centralizar as configurações e facilitar o controle dos dados dos usuários.

b. Disposições legais relevantes

124. Como mencionado acima,[63] como um dos principais princípios relativos ao processamento de dados pessoais, o Artigo 5 (1) (a) GDPR estipula que os dados pessoais devem ser processados de forma lícita, justa e, especialmente crucial a este respeito, de forma transparente em relação ao envolvido ("licitude, justiça e transparência"). De acordo com o princípio de responsabilidade conforme o Artigo 5 (2) da GDPR, os controladores são obrigados a mostrar quais medidas estão tomando para tornar suas atividades de processamento não apenas lícitas e justas, mas também transparentes. Além disso, os princípios de minimização conforme o Artigo 5 (1) (c) e proteção de dados por projeto e default conforme o Artigo 25 GDPR são relevantes neste caso de uso.

c. Padrões de design enganosos

i. Padrões baseados no conteúdo

125. A primeira questão que os usuários encontram neste contexto é onde realmente encontrar configurações que lidem com a proteção de dados. Os usuários podem ler o aviso de proteção de dados e então decidir fazer mudanças relacionadas ao processamento de seus dados pessoais. Eles também podem desejar fazê-lo sem ter lido o aviso, apenas através de seu uso regular da mídia social, por exemplo, quando percebem que uma informação publicada em uma plataforma de mídia social (por exemplo, uma foto na praia com a família) é compartilhada com um grupo indesejado de pessoas (por exemplo, colegas de trabalho). Em qualquer caso, o princípio da transparência exige que as opções de configuração sejam facilmente acessíveis, bem como que estejam disponíveis de forma compreensível. Isto poderia ser alcançado através da centralização das configurações de dados e privacidade em um único lugar, usando um URL auto-explicativo, como [social-network.com]/data-settings.

126. Há vários padrões de design relacionados a esta questão que dificultam aos usuários encontrar as configurações. Portanto, os projetistas de plataformas de mídia social devem estar atentos para evitar estes padrões de design enganosos.

Sobrecarga - Demasiadas opções (Anexo I lista de verificação 4.1.3)

127. As configurações de proteção de dados precisam ser facilmente acessíveis e ordenadas de forma lógica. As configurações relacionadas ao mesmo aspecto da proteção de dados devem, de preferência, estar localizadas em um único e proeminente local. Caso contrário, os usuários estarão diante de demasiadas páginas para verificar e rever o que os sobrecarrega nas configurações de suas preferências de proteção de dados. De fato, diante de um ***excesso de opções*** para escolher, pode deixá-los incapazes de fazer qualquer escolha ou fazê-los ignorar algumas configurações, finalmente desistindo ou perdendo as configurações de suas preferências de proteção de dados. Isto infringe os princípios de transparência e justiça. Em particular, pode infringir o Artigo 12 (1) GDPR, pois ou torna difícil um controle específico relacionado à proteção de dados, já que está espalhado por várias páginas, ou faz com que a diferença entre as diferentes opções fornecidas aos usuários não seja clara.

> **Exemplo 36:** Os usuários provavelmente não sabem o que fazer quando o menu de uma plataforma de mídia social contém múltiplas abas que tratam da proteção de dados: "*proteção de dados*", "*segurança*", "*conteúdo*", "*privacidade"*, "*suas preferências*".

128. Neste exemplo, os títulos das guias não indicam obviamente o que os usuários podem esperar na página associada ou que todos eles se relacionam com a proteção de dados, especialmente quando

uma das guias leva especificamente este nome. Isto pode criar o risco de impedir que os usuários façam mudanças. Por exemplo, se eles quiserem restringir ou ampliar o número de pessoas que podem ver as imagens que carregaram, os nomes das abas podem levá-los a clicar em "segurança", se os usuários acharem que há alguns riscos de segurança em

[63] Ver acima, para. 1, 9, 10, 14-16.

ter seus dados acessíveis ao público; "conteúdo", pois os usuários desejam definir a visibilidade de sua postagem; ou "privacidade", pois esta noção específica está diretamente relacionada ao que as pessoas querem compartilhar com outros. Isto significa que estes títulos não são suficientemente claros no que diz respeito à ação que os usuários gostariam de realizar. Em particular, os termos "proteção de dados" e "privacidade" são freqüentemente usados como sinônimos e, portanto, são especialmente confusos se apresentados como seções diferentes.

Deixado no escuro - Informações contraditórias (Anexo I lista de verificação 4.6.2)

129. Como já descrito no exemplo 12 e ilustrado no exemplo a seguir, os usuários também podem receber ***informações conflitantes*** dentro da estrutura das configurações de proteção de dados.

> **Exemplo 37:** O usuário X desliga o uso de sua geolocalização para fins publicitários. Após clicar na chave múltipla que permite fazê-lo, aparece uma mensagem dizendo *"Desligamos sua geolocalização, mas sua localização ainda será usada".*

Sobrecarga - Labirinto de privacidade (Anexo I lista de verificação 4.1.2)

130. Quando os usuários mudam um ambiente de proteção de dados, o princípio de justiça também exige que os provedores de mídia social informem os usuários sobre outros ambientes que são similares. Se tais configurações estiverem espalhadas por páginas diferentes e não conectadas da plataforma de mídia social, os usuários provavelmente perderão um ou vários meios para controlar um aspecto de seus dados pessoais. Os usuários esperam encontrar configurações relacionadas umas com as outras.

> **Exemplo 38:** Tópicos relacionados, como as configurações sobre compartilhamento de dados pelo provedor de mídia social com terceiros e vice-versa, não são disponibilizados nos mesmos espaços ou em espaços fechados, mas sim em abas diferentes do menu de

131. Não há uma "abordagem de tamanho único" quando se trata do número médio de passos ainda suportáveis para os usuários de plataformas de mídia social ao mudar um ambiente. Ao mesmo tempo, um número maior de passos pode desencorajar os usuários de finalizar a mudança ou fazê-los perder partes dela, especialmente se eles quiserem fazer várias mudanças. Impedir de tal forma a vontade dos usuários infringe os princípios de equidade do Artigo 5 (1) (a) GDPR. Além disso, a alteração das configurações está intimamente relacionada ao exercício dos direitos do sujeito dos dados.[64] A alteração de uma configuração relacionada aos dados, como corrigir o nome ou apagar o ano de formatura, pode ser considerada um exercício do direito de retificação, respectivamente direito de apagamento, para estes dados específicos. O número de etapas necessárias deve, portanto, ser o mais baixo possível. Embora possa variar, um número excessivo de etapas dificulta os usuários e, portanto, viola o princípio da justiça, bem como os artigos 12 (1) e (2) do GDPR.

Fickle - Descontinuidade da língua (Anexo I lista de verificação 4.5.4)

132. Com relação à informação transparente, os projetistas de plataformas de mídia social também precisam ser cuidadosos para evitar padrões de design enganosos baseados em conteúdo listados no caso 2a, tais como ***descontinuidade de linguagem.*** Não disponibilizar as páginas de definição (ou partes delas) no idioma escolhido pelos usuários para a plataforma de mídia social torna mais difícil para eles entender o que podem mudar e, portanto, definir suas preferências.

[64] Veja abaixo, Utilize os casos 4 e 5, ou seja, as partes 3.4. e 3.5. destas Diretrizes.

Fickle - Interface Inconsistente (Anexo I lista de verificação 4.5.3)

133. Neste contexto, outra questão ocorre quando as plataformas de mídia social oferecem aos usuários opções amigáveis de proteção de dados, mas não os informam sobre isso de maneira clara. Este pode ser o caso quando a plataforma de mídia social difere repentinamente de seu padrão usual de design. Tal ***Interface Inconsistente*** ocorre quando uma interface não é consistente em diferentes contextos ou com as expectativas dos usuários. Estas diferenças podem levar os usuários a não encontrar o controle ou informação desejada ou a interagir com um elemento da interface fora dos hábitos, mesmo que esta interação leve a fazer uma escolha de proteção de dados que os usuários não desejam.

> **Exemplo 39:** Em toda a plataforma de mídia social, nove em cada dez opções de configuração de proteção de dados são apresentadas na seguinte ordem:
>
> - opção mais restritiva (ou seja, compartilhar o mínimo de dados com outros)
>
> - opção limitada, mas não tão restritiva quanto a primeira
>
> - opção menos restritiva (ou seja, compartilhar a maioria dos dados com outros).
>
> Os usuários desta plataforma estão acostumados a que suas configurações de proteção de dados sejam apresentadas nesta ordem. No entanto, esta ordem não é aplicada na última configuração onde a escolha da visibilidade dos aniversários dos usuários é mostrada na seguinte ordem:
>
> - *Mostrar meu aniversário inteiro: 15 de janeiro de 1929* (= opção menos restritiva)
>
> - *Mostrar apenas dia e mês: 15 de janeiro* (= opção limitada, mas não a mais restritiva)
>
> - *Não mostrar aos outros meu aniversário* (= opção mais restritiva).

134. No exemplo, as três escolhas na última configuração são apresentadas em uma ordem diferente das configurações anteriores. Os usuários que mudaram anteriormente suas outras configurações provavelmente estarão acostumados à ordem "usual" de configurações de um a nove. Na última configuração, eles estão tão acostumados a esta ordem que instintivamente escolhem a primeira opção, assumindo que esta deve ser a mais restritiva. Organizar as opções de uma configuração de proteção de dados de forma tão diferente das outras na mesma plataforma de mídia social é uma ***Interface Inconsistente***, pois ela joga com o que os usuários estão acostumados e suas expectativas. Isto pode levar à confusão ou deixar os usuários a pensar que fizeram a escolha que queriam quando, na realidade, este não é o caso.

ii. Padrões baseados em interfaces

135. A segunda questão que se encontra no contexto das configurações de proteção de dados é que as configurações podem infringir o princípio da proteção de dados por padrão. O artigo 25 (1) GDPR exige que os controladores tomem medidas apropriadas para implementar os princípios de proteção de dados, tais como a minimização de dados (artigo 5 (1) (c) GDPR). Estas disposições não são respeitadas quando as configurações sobre compartilhamento de dados pessoais são pré-definidas para uma das opções mais invasivas em vez da opção menos invasiva.

Pular - Aconchego Enganoso (Anexo I lista de verificação 4.2.1)

> **Exemplo 40:** Entre as opções de visibilidade de dados *"visível para mim", "para meus amigos mais próximos" "para todas as minhas conexões",* e *"público"*, a opção do meio *"para todas as minhas conexões"* é pré-definida. Isto significa que todos os usuários conectados a eles

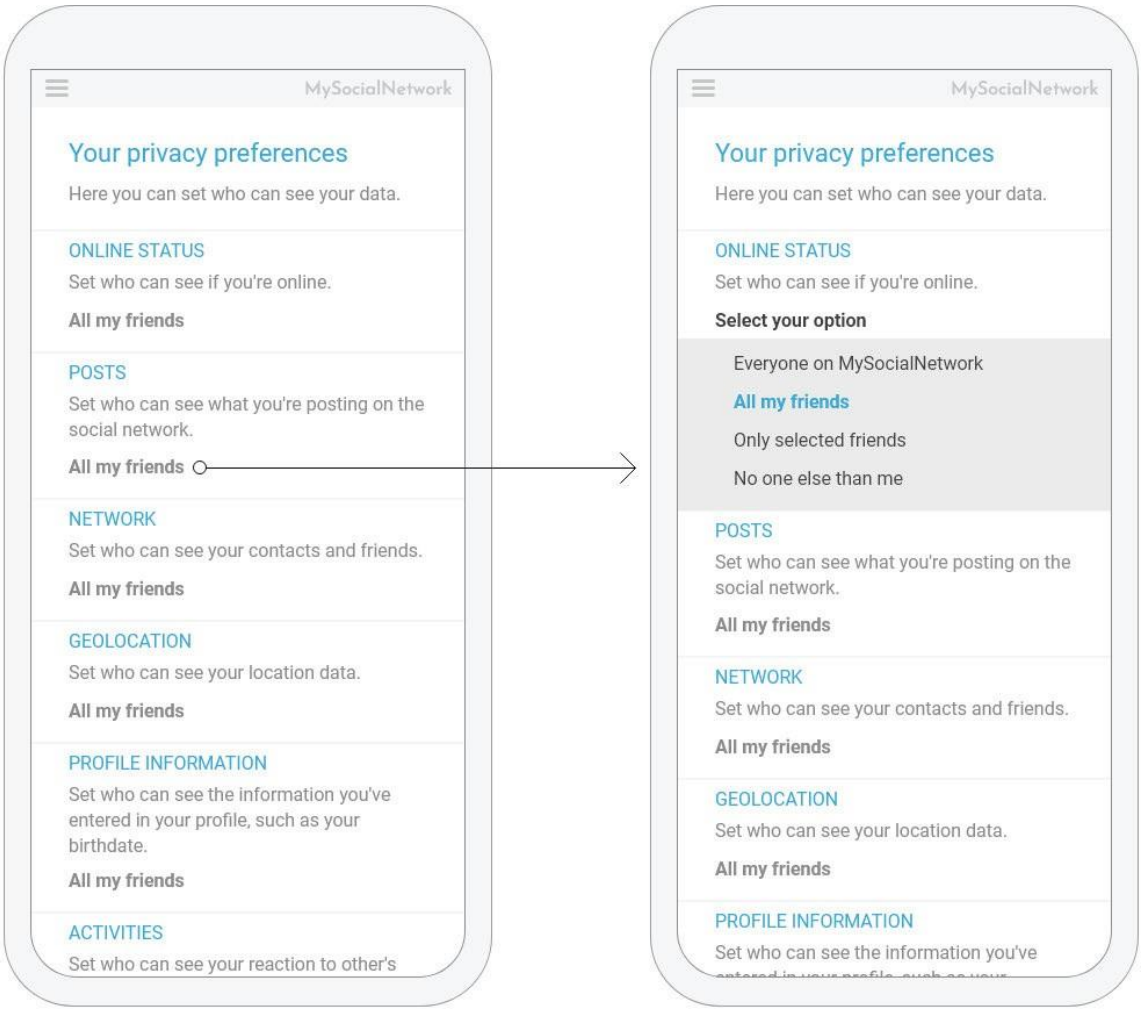
informações inseridas para a inscrição na plataforma de mídia social, tais como seu endereço de e-mail ou data de nascimento.

136. Os provedores de mídia social podem argumentar que o cenário menos invasivo derrotaria o objetivo que os usuários de uma determinada plataforma de mídia social têm, por exemplo, serem encontrados por pessoas desconhecidas para encontrar um novo amigo, namorado ou emprego. Embora isto possa ser verdade para alguns ambientes particulares, os provedores de mídia social precisam ter em mente que o fato de os usuários carregarem certos dados na rede não constitui consentimento para compartilhar estes dados com outros.[65] Quando os provedores de mídia social se desviam da proteção de dados por padrão, eles precisarão estar atentos para informar adequadamente os usuários sobre isso. Isto significa que os usuários precisam saber qual é a configuração padrão, que há opções menos invasivas disponíveis e para onde na plataforma eles precisam ir para fazer mudanças. No exemplo dado, isto significa que quando a opção "*para meus amigos mais próximos*" é pré-definida para contribuições que os usuários postam ativamente na plataforma de mídia social, eles devem ser mostrados onde mudar esta configuração. Entretanto, a pré-definição da visibilidade para "*todas as conexões dos usuários*" (ou mesmo para o público em geral) constitui uma ***comodidade enganosa,*** especialmente quando é aplicada aos dados que o provedor de mídia social exige dos usuários para criar uma conta, como o endereço de e-mail ou sua data de nascimento. Como descrito no caso 1 para. 55, esta prática infringe o artigo 25 (2) da GDPR.

[65] Por exemplo, sua data de nascimento, ver parágrafo. 58 acima.

Agitação - Escondida à vista (Anexo I lista de verificação 4.3.2)

137. Os padrões de design enganoso ***Escondidos em Clara Visão*** e ***Enganosos*** podem ser facilmente combinados quando se trata da seleção de opções relacionadas à proteção de dados, como ilustrado no exemplo 9 para o processo de inscrição, e abaixo quando os usuários querem mudar suas preferências de proteção de dados enquanto usam as mídias sociais.



Exemplo 41: Neste exemplo, quando os usuários querem gerenciar a visibilidade de seus dados, eles têm que ir na aba *"preferência de privacidade"*. As informações para as quais eles podem definir sua preferência são listadas ali. Entretanto, a forma como a informação é exibida não torna óbvia a forma de alterar as configurações. De fato, os usuários têm que clicar na opção de visibilidade atual para acessar um menu suspenso do qual eles podem selecionar a opção de sua preferência.

138. Mesmo que a mudança das preferências esteja disponível nesta aba, ela está ***oculta à vista,*** pois o menu suspenso não é diretamente visível para os usuários que têm que adivinhar que clicando na opção atual abrirá algo. De fato, não há nenhuma pista visual usual (texto sublinhado, seta para baixo) sobre a possibilidade de interagir e abrir o menu suspenso. Esta prática específica é injusta para os usuários e poderia participar de uma falha geral no cumprimento do princípio de justiça do Artigo 5 (1) (a) GDPR. Além disso, se as opções fossem pré-selecionadas por padrão, o padrão de design enganoso ***Snugness Deceptive*** poderia também ser observado, como descrito no parágrafo

acima. 128.

Fickle - Descontextualização (Anexo I lista de verificação 4.5.2)

139. ***A descontextualização*** acontece quando uma informação ou controle relacionado à proteção de dados está localizado em uma página que está fora do contexto, de modo que é improvável que os usuários a encontrem, pois não seria intuitivo procurá-la naquela página específica.

> **Exemplo 42:** As configurações de proteção de dados são difíceis de encontrar na conta do usuário, pois no primeiro nível, não há capítulo de menu com um nome ou título que conduza nessa direção.

140. Neste exemplo, os usuários não são guiados para as configurações de proteção de dados porque não são utilizados termos significativos e claros para indicar onde estes se encontram na plataforma de mídia social. De fato, o termo *"Segurança"* cobre apenas uma fração do que pode ser esperado das configurações de proteção de dados. Portanto, não é intuitivo para os usuários consultar este menu para encontrar tais configurações. Esta falta de transparência torna o acesso à informação mais difícil do que deveria e pode ser considerado como uma violação do Artigo 12 (1) GDPR, e potencialmente do Artigo 12 (2) GDPR se essas configurações estiverem relacionadas ao exercício de um direito.

> **Exemplo 43: A** alteração do cenário é dificultada, pois na versão desktop da plataforma de mídia social, o botão "*salvar*" para registrar suas alterações não é visível com todas as opções, mas somente no topo do submenu. É provável que os usuários o ignorem e assumam erroneamente que suas configurações são salvas automaticamente, portanto, mudando para outra página sem clicar no botão "*salvar*". Este problema não ocorre nas versões app e mobile. Portanto, cria confusão adicional para os usuários que passam da versão móvel/app para a versão desktop, e pode fazê-los pensar que só podem alterar suas configurações na versão móvel ou no aplicativo.

141. Uma vez que os usuários tenham encontrado as configurações de proteção de dados e definido suas escolhas, eles não poderão ser impedidos de fazê-lo. Uma vez que os usuários tenham feito uma mudança, a maneira de salvá-la tem que ser óbvia, quer isto aconteça assim que os usuários ajustarem uma configuração ou precise de uma confirmação clicando em um elemento específico da interface, como um botão "salvar". Além disso, o princípio de justiça sob o Artigo 5 (1) (a) GDPR exige que os provedores de mídia social sejam consistentes em toda sua plataforma, especialmente através de diferentes dispositivos. Este não é o caso quando a interface usa um padrão de design enganoso, como descrito nos exemplos acima.

d. As melhores práticas

Diretório de proteção de dados: Para fácil orientação através da seção diferente do menu, forneça aos usuários uma página facilmente acessível de onde todas as ações relacionadas à proteção de dados (por exemplo, configurações) e informações estejam acessíveis. Esta página pode ser encontrada no menu principal de navegação do provedor de mídia social, a conta do usuário, através da política de privacidade, etc.

Opções a granel: Colocar opções que têm a mesma finalidade de processamento juntas, para que os usuários possam mudá-las mais facilmente, deixando ainda aos usuários a possibilidade de fazer mudanças mais granulares. Se as plataformas de mídia social apresentarem opções em massa, estas não devem conter elementos inesperados ou não relacionados (por exemplo, elementos com finalidades diferentes). Se o processamento exigir consentimento, as opções em massa devem estar de acordo com as Diretrizes da EDPB sobre consentimento, especialmente o parágrafo. 42-44.

Atalhos: ver caso de uso 1 para definição (p. 22). *(por exemplo, quando os usuários são informados*

URL auto-explicativa: páginas relacionadas a configurações de proteção de dados ou informações devem usar um endereço web que reflita claramente seu conteúdo. Por exemplo, uma página centralizando o controle de proteção de dados poderia ter um URL tal como [social-network.com]/data-settings.

Palavras coerentes: ver caso de uso 1 para definição (p.

22). **Fornecer definições**: ver caso de uso 1 para definição

(p. 22). **Uso de exemplos: ver caso de** uso 1 para definição

(p. 22).

Navegação pegajosa: ver caso de uso 2a para definição (p. 28).

Notificações: ver caso de uso 2c para definição (p. 32).

3.4 Manter-se direito às mídias sociais: Direitos do sujeito dos dados

Usar o caso 4: Como fornecer funções adequadas para o exercício dos direitos do sujeito dos dados

a. Descrição do contexto

142. Utilizar uma plataforma de mídia social significa tirar proveito de suas funções ao longo dos objetivos declarados pelo fornecedor da mídia social. Isto também significa que os usuários podem exercer seus direitos de proteção de dados. Eles são elementos-chave da proteção de dados e do controle das próprias informações, independentemente de os dados serem fornecidos direta e conscientemente pelos indivíduos, fornecidos pelos indivíduos em virtude do uso do serviço ou do dispositivo, ou inferidos a partir da análise dos dados fornecidos pelo indivíduo em questão.[66] A quantidade de dados pessoais que flui por toda a plataforma requer que os usuários possam controlar seus dados com a ajuda dos direitos fornecidos pela GDPR, de forma clara e intuitiva. A EDPB tem explicado estes conceitos em várias diretrizes.[67] O exercício dos direitos deve estar disponível desde o início até o final da utilização da plataforma e, em alguns casos, mesmo depois que os usuários tenham decidido deixar a plataforma e o controlador ainda não tenha apagado seus dados. Os não usuários da plataforma também precisam estar habilitados a exercer os direitos do sujeito dos dados relativos ao processamento de seus dados. É claro que, em alguns casos, nem todos os direitos do envolvido estão disponíveis, dependendo da base legal para o processamento dos dados. O provedor de mídia social também deve, portanto, explicar claramente porque certos direitos não são aplicáveis e porque alguns deles podem ser limitados. Como mencionado acima e nos capítulos anteriores, o uso dos direitos deve ser operacionalizado. A automação, assim como outras funcionalidades das plataformas de mídia social devem ser utilizadas para facilitar o exercício dos direitos.

b. Disposições legais relevantes

143. A GDPR descreve sete direitos diferentes que os sujeitos dos dados podem exercer de acordo com certas condições (por exemplo, base legal do processamento, etc.). O artigo 15 da GDPR permite aos sujeitos dos dados saber se

[66] Ver Diretrizes do Grupo de Trabalho do Artigo 29 sobre o direito à portabilidade de dados sob o Regulamento 2016/679, WP242 rev.01, p. 10, https://ec.europa.eu/newsroom/article29/items/611233/en.
[67] Diretrizes sobre o direito à portabilidade de dados e Diretrizes EDPB 05/2019 sobre os critérios do direito a ser esquecido nos casos dos motores de busca sob o GDPR (parte 1) - versão adotada após consulta pública, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be- forgotten-search-engines_en.

Os dados pessoais que lhes dizem respeito são processados e para acessá-los, ou seja, para obter mais informações sobre seu processamento, bem como para receber uma cópia desses dados. O artigo 16 da GDPR detalha o direito de retificação, permitindo às pessoas em questão atualizar os dados pessoais que o responsável pelo tratamento processa. O direito de apagamento nos termos do artigo 17 da GDPR permite às pessoas em causa obter o apagamento dos dados pessoais que lhes dizem respeito. O direito à restrição do processamento de acordo com o Artigo 18 GDPR dá aos titulares dos dados a possibilidade de interromper temporariamente o processamento de seus dados pessoais. O artigo 20 da GDPR introduz o direito à portabilidade dos dados, permitindo às pessoas em questão receber seus dados pessoais e transmiti-los a outro controlador.[68] Os titulares dos dados também têm o direito de se opor ao processamento de seus dados pessoais, conforme estabelecido no Artigo 21 GDPR. Finalmente, o artigo 22 da GDPR dá às pessoas em causa o direito de não se oporem a uma decisão baseada unicamente no processamento automatizado.[69]

144. A EDPB salienta que nem todos esses direitos serão aplicáveis a todas as plataformas de mídia social, dependendo de sua base legal e dos objetivos de processamento de dados pessoais e tipos de serviços prestados. As diferenças devem ser explicadas pelo controlador, de acordo com o artigo 12 da GDPR. Isto significa que as informações sobre os direitos aplicáveis devem ser concisas e claras para os usuários, incluindo a razão pela qual certos direitos não se aplicam. Tal explicação poderia limitar a quantidade de comunicação com os usuários quando eles estão tentando exercer alguns deles. O exercício do direito deve ser fácil e acessível de acordo com o Artigo 12 (2) e a resposta deve ser dada sem demora indevida, conforme exigido pelo Artigo 12 (3) GDPR. Da mesma forma, a plataforma de mídia social deve explicar por que certos pedidos não podem ser atendidos e informar sobre a possibilidade de apresentar uma reclamação a uma autoridade supervisora designada, conforme o Artigo 12 (4) GDPR. Assim, os seguintes padrões enganosos podem não ser aplicáveis a todos os direitos mencionados acima. O direito de apagamento é discutido em detalhes no próximo capítulo.

c. Padrões de design enganosos

i. Padrões baseados no conteúdo

Obstrução - Ponto morto (Anexo lista de verificação I 4.4.1)

145. O padrão de design enganoso do ***beco sem saída*** pode impactar diretamente na facilidade de acesso ao exercício dos direitos. Quando os links redirecionados para os meios de exercício de um direito são quebrados ou faltam explicações claras sobre como exercer um direito, os usuários não poderão exercê-lo adequadamente, o que infringe o Artigo 12 (2) GDPR.

> **Exemplo 44:** Os usuários clicam em "*exercer meu direito de acesso*" no aviso de privacidade, mas são redirecionados para seu perfil, que não oferece nenhuma característica relacionada ao exercício do direito.

146. O exemplo acima mencionado de um padrão de design enganoso delineia a necessidade de fornecer aos usuários uma maneira clara e intuitiva de exercer seus direitos de acordo com o Artigo 12 (1) e (2) GDPR, pois de outra forma eles poderiam não ser capazes de exercê-los. Não é suficiente confirmar aos usuários que eles têm direitos sobre os dados conforme exigido pelo Artigo 12 (1) GDPR (incluindo a forma de comunicação) e especificamente pelos Artigos 13 (2) (b) e 14 (2) (c) GDPR. Os usuários também devem ser capazes de exercê-los facilmente, de preferência de forma integrada na interface da plataforma, por exemplo, fornecendo um formulário dedicado. Isto também tornaria a experiência do usuário com uma plataforma mais positiva - visto que o provedor

se esforçou para se adaptar às expectativas dos usuários em relação ao processamento e controle legal de dados pessoais.

[68] Este direito está mais desenvolvido nas Diretrizes sobre o direito à portabilidade de dados.
[69] Ver também as Diretrizes do Grupo de Trabalho do Artigo 29 sobre a tomada de decisões e perfis automatizados individuais para os fins do Regulamento 2016/679, wp251rev.01, p. 19 e seguintes, https://ec.europa.eu/newsroom/article29/items/612053/en.

seus dados, combinando o exercício dos direitos com outras funcionalidades do serviço. Quando o serviço de plataforma de mídia social permite uma comunicação bidirecional entre usuários, assim como entre o controlador e os usuários, não há razão para o controlador limitar seu canal de comunicação para a facilitação de solicitações de dados a um meio de comunicação separado, como o e-mail. Ao mesmo tempo, os sujeitos dos dados não devem ser forçados a vir até a plataforma para se comunicar com o controlador.[70] Além disso, os controladores não podem limitar este direito do envolvido ao direito de cópia, mas, em vez disso, precisam garantir que eles também forneçam as informações mencionadas pelo Artigo 15 (1) GDPR aos usuários que solicitem acesso aos seus dados.[71]

Fickle - Descontinuidade do idioma (Anexo I lista de verificação 4.5.4)

> **Exemplo 45:** Ao clicar em um link relacionado ao exercício dos direitos do sujeito dos dados, as seguintes informações não são fornecidas no(s) idioma(s) oficial(is) do estado do país do usuário, enquanto que o serviço é. Ao invés disso, os usuários são redirecionados para uma

147. Tendo em mente o princípio de transparência previsto nos artigos 5 (1) (a) e 12 (1) GDPR, os usuários devem receber todas as informações sobre seus direitos de forma clara e clara, compreensível. Isto também deve estar relacionado à localização dos usuários e ao idioma utilizado naquele país ou jurisdição em que o serviço é oferecido. O fato de os usuários confirmarem sua capacidade de usar um idioma estrangeiro de qualquer forma não libera o controlador de suas obrigações. O mesmo se aplica quando tal conhecimento de outros idiomas compreendidos pelos usuários pode ser inferido a partir de suas atividades. As informações devem ser relevantes e úteis aos usuários que exercem seus direitos.

Esquerda na escuridão - texto ou informações ambíguas (Anexo I lista de verificação 4.6.3)

148. No contexto dos direitos do sujeito dos dados, os usuários também podem ser confrontados com o padrão de design enganoso, com ***palavras ou informações ambíguas***, como mostrado no exemplo a seguir.

> **Exemplo 46:** A plataforma de mídia social não declara explicitamente que os usuários na UE têm o direito de apresentar uma reclamação a uma autoridade supervisora, mas apenas menciona que em alguns - sem mencionar quais - países, existem autoridades de proteção de dados com as quais o provedor de mídia social coopera em relação às reclamações.

149. Os provedores de mídia social também precisam estar atentos para evitar a ***formulação ambígua ou o*** padrão de design enganoso de ***informações*** ao informar os sujeitos dos dados sobre seus direitos. Dar informações aos usuários de uma forma que os torne inseguros sobre como seus dados serão processados ou como ter algum controle sobre seus dados e, portanto, como exercer seus direitos, viola o princípio da transparência. Além disso, a formulação vaga não é uma linguagem concisa como exigido pelo Artigo 12 (1) GDPR e pode tornar as informações fornecidas ao envolvido incompletas, o que poderia ser considerado uma violação do Artigo 13 GDPR. O exemplo acima mencionado também mostra uma violação do Artigo 13 (2) (d) GDPR que exige que os controladores forneçam aos sujeitos dos dados informações sobre seu direito de apresentar um

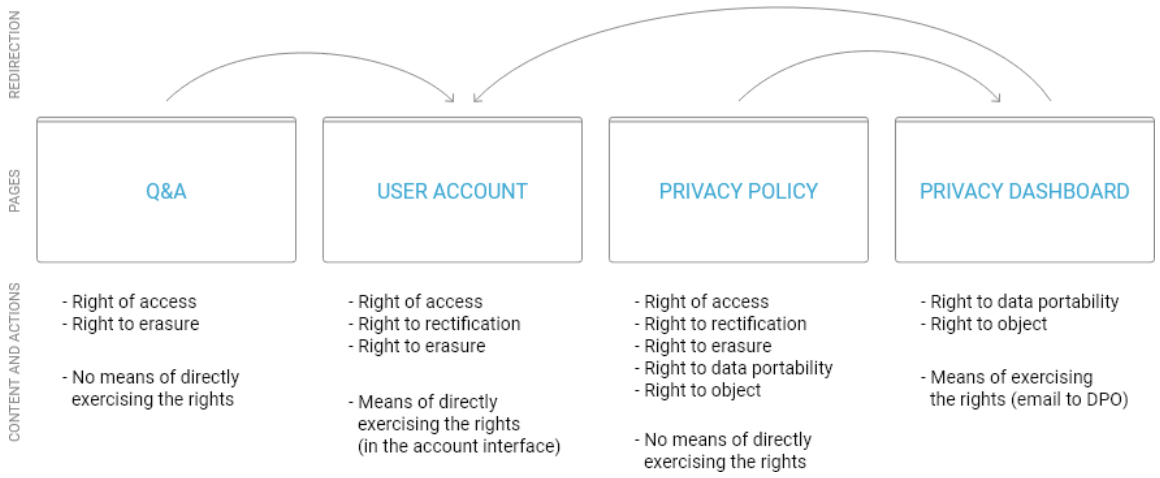
[70] Ver Diretrizes EDPB 01/2022 sobre direitos de acesso aos dados - direito de acesso, para. 136, versão 1.0, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[71] Ver Diretrizes EDPB 01/2022, para. 131, 142, 145.

reclamação junto a uma autoridade de supervisão. Por extensão, isto também é contrário ao Artigo 12 (2) GDPR porque o provedor da mídia social não facilita o exercício do direito de apresentar uma reclamação.

ii. Padrões baseados em interfaces

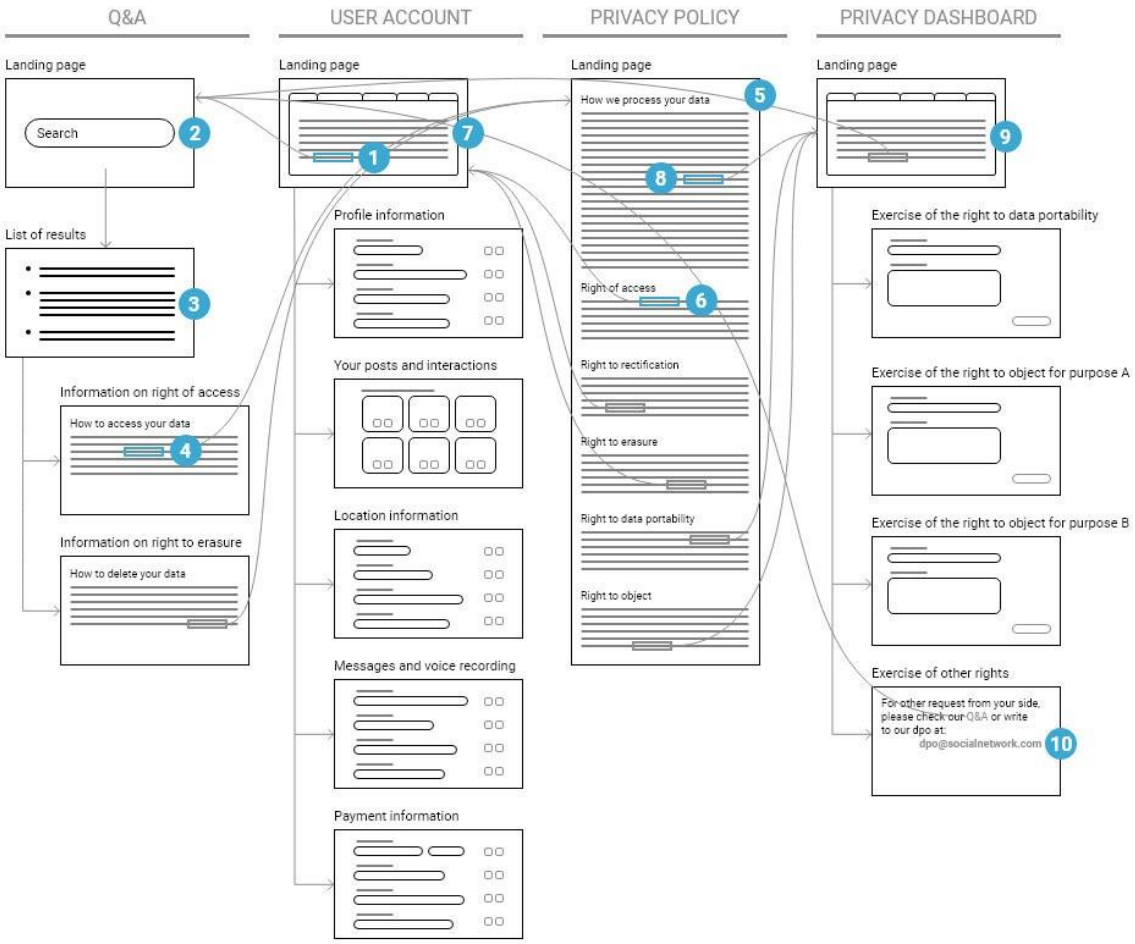
Sobrecarga - Labirinto de Privacidade (Anexo I lista de verificação 4.1.2)

150. Como descrito anteriormente no caso 3b, o número de passos necessários para receber as informações relevantes sobre proteção de dados não deve ser excessivo, nem o número de passos para alcançar os direitos do sujeito dos dados.[72] Assim, os usuários devem sempre ser capazes de alcançar rapidamente o site de exercício dos direitos, não importando de que ponto de partida eles vieram e onde a plataforma de mídia social localizou este recurso. Os provedores de mídia social devem, portanto, pensar cuidadosamente sobre as diferentes situações das quais os usuários gostariam de exercer seus direitos e projetar o acesso ao local onde eles podem fazê-lo de acordo. Isto significa que vários caminhos para chegar a um direito do sujeito dos dados podem ser criados e disponibilizados em uma plataforma de mídia social. Entretanto, cada caminho deve facilitar o acesso ao exercício dos direitos e não deve interferir em outro caminho. Caso contrário, seria considerado um padrão de desenho enganoso do ***Privacy Maze***, como ilustrado nos exemplos 47 e 48, ao contrário do Artigo 12 (2) GDPR.



Exemplo 47: Aqui, as informações relacionadas aos direitos de proteção de dados estão disponíveis em pelo menos quatro páginas. Mesmo que a política de privacidade informe sobre todos os direitos, ela não redireciona para as páginas relevantes para cada um deles. Por outro lado, quando os usuários visitam sua conta, eles não encontrarão nenhuma informação sobre alguns dos direitos que podem exercer. Este ***Labirinto de Privacidade*** força os usuários a vasculhar muitas páginas a fim de encontrar onde exercer cada direito e,

[72] Ver acima, para. 123.



Exemplo 48: Neste exemplo, os usuários desejam atualizar alguns de seus dados pessoais, mas não encontram uma maneira de fazê-lo em sua conta. Eles clicam em um link (1) redirecionando-os para a página de Perguntas e Respostas, onde eles inserem sua pergunta (2). Vários resultados aparecem (3), alguns relacionados com os direitos de acesso e exclusão. Após verificar todos os resultados, eles clicam (4) no link disponível na página "Como acessar seus dados". Ele os redireciona para a política de privacidade (5). Lá, eles encontram informações sobre direitos adicionais. Após ler estas informações, eles clicam (6) no link associado ao exercício do direito de retificação que os redireciona para a conta do usuário (7). Insatisfeitos, eles voltam à política de privacidade e clicam em um link geral "Envie-nos um pedido" (8). Isto traz os usuários ao seu painel de controle de privacidade (9). Como nenhuma das opções disponíveis parece corresponder às suas necessidades, os

151. Ambos os exemplos ilustram caminhos particularmente longos e cansativos para exercer os próprios direitos. Quando os meios para exercer direitos diferentes não estão localizados no mesmo espaço, mas uma página listando todos os direitos do sujeito dos dados está disponível, o último deve ser redirecionado precisamente para esses espaços diferentes, não apenas para um ou parte deles, como ilustrado no exemplo 47. O outro exemplo mostra uma viagem onde os usuários não encontram o meio de exercer facilmente o direito específico que desejam, ou seja, o direito à retificação, pois o local onde ela é comumente realizada, ou seja, a conta do usuário, não fornece o meio para fazê-lo.

Procurando outra forma de exercer este direito, não conseguem encontrar uma forma específica correspondente e têm que recorrer a um meio geral fornecido no painel de privacidade.

152. Quando vários caminhos para o exercício de um direito tiverem sido projetados, deve ser sempre fácil para os usuários encontrar a visão geral sobre os direitos do sujeito dos dados. As políticas de privacidade devem ser claras e podem servir como uma das portas de entrada para as páginas onde os usuários podem exercer seus direitos. Este documento deve incluir todos os direitos que são aplicáveis. Se algum deles não estiver disponível devido a limitações legais ou técnicas, isto também deve ser explicado, para que os usuários sejam devidamente informados. A compreensão das limitações das operações de processamento, seja devido à sua base ou às salvaguardas adotadas pelos controladores, é útil não apenas para os usuários. Também limita os casos em que um provedor de mídia social tem que explicar por que não pode atender a um pedido de direitos do sujeito dos dados feito pelos usuários.

Agitação - Escondida à vista (Anexo I lista de verificação 4.3.2)

153. Afetar a capacidade dos usuários de alcançar o lugar onde exercer seu direito também pode ser feito tornando as informações relacionadas ou links dificilmente visíveis usando o padrão de design enganoso ***Escondido em Vista Simples.***

> **Exemplo 49:** O parágrafo sob o subtítulo "direito de acesso" na política de privacidade explica que os usuários têm o direito de obter informações sob o Artigo 15 (1) GDPR. Entretanto, menciona apenas a possibilidade dos usuários de receberem uma cópia de seus dados pessoais. Não há nenhum link direto visível para exercer o componente de cópia do direito de acesso de acordo com o Artigo 15 (3) GDPR. Ao contrário, as três primeiras palavras em "Você pode ter uma cópia de seus dados pessoais" estão ligeiramente sublinhadas. Ao pairar sobre estas palavras com o mouse dos usuários, uma pequena caixa é exibida com um

154. Acrescentando à seção anterior, qualquer meio criado pelo controlador para o exercício dos direitos deve ser facilmente acessível. Esta regra não pode ser subestimada. Uma ação do controlador, como descrita acima, pode ser vista apenas como um esforço para dificultar o exercício de direitos pelos usuários, o que infringe o Artigo 12 (2) GDPR. Os controladores, não importando suas razões, não devem inibir tal solicitação. Após um exame mais detalhado por uma autoridade de supervisão em um caso específico, isto poderia contribuir para uma violação da GDPR levando a sancionar o controlador.

Fickle - Interface Inconsistente (Anexo I lista de verificação 4.5.3)

> **Exemplo 50:** A plataforma de mídia social oferece diferentes versões (desktop, aplicativo, navegador móvel). Em cada versão, as configurações (que levam a acessos/objetos etc.) são exibidas com um símbolo diferente, deixando os usuários que alternam entre as versões

155. Confrontados com interfaces através de diferentes dispositivos que transmitem as mesmas informações através de vários significantes visuais, é provável que os usuários demorem mais tempo ou tenham dificuldades para encontrar controles que conhecem de um dispositivo para outro. No exemplo acima, isto se deve ao uso de símbolos ou ícones diferentes para direcionar os usuários para as configurações. A confusão dos usuários de tal forma poderia ser considerada conflitante com a facilitação dos direitos do sujeito dos dados, conforme estabelecido no Artigo 12 (2) GDPR.

Obstrução - Mais longa do que o necessário (Anexo I lista de verificação 4.4.2)

156. Finalmente, qualquer tentativa de fazer o exercício de um direito ***mais longo do que o necessário*** pode ser considerada contrária ao GDPR.

> **Exemplo 51:** Quando os usuários escolhem apagar o nome e o local de sua escola secundária ou a referência a um evento que participaram e compartilharam, surge uma segunda janela pedindo para confirmar essa escolha ("*Você realmente quer fazer isso? Por que você quer*

157. Da mesma forma que a quantidade de camadas em uma política de privacidade (use o caso 2a) e o número de passos para alcançar ou alterar uma configuração (use o caso 3b), a quantidade de passos ou cliques que os usuários precisam dar para exercer um direito não deve ser excessiva. Isto, naturalmente, depende da complexidade das operações conduzidas pelo controlador, levando em consideração o contexto específico. No entanto, não seria razoável exigir que os usuários tomem um número elevado de ações desnecessárias para concluir o exercício de seu direito. Por exemplo, os usuários não devem ser desencorajados por perguntas adicionais, tais como se realmente querem exercer este direito ou quais são as razões para tal solicitação. Na maioria dos casos, eles devem ser capazes de simplesmente exercer seu direito, sem que sua motivação seja posta em questão. Tais práticas, ilustradas no exemplo acima, podem ser consideradas contrárias ao Artigo 12 (2) GDPR, pois o controlador dificulta o exercício dos direitos com passos desnecessários. Isto, naturalmente, não impede que o controlador receba feedback, fazendo perguntas adicionais posteriormente com o objetivo de melhorar o serviço. Ao fazer esta pergunta posteriormente, respondê-la dependeria apenas da vontade dos usuários e não seria confundida com uma exigência de exercício de um direito.

d. As melhores práticas

Exercício do formulário de direitos: para facilitar aos usuários o exercício de seus direitos GDPR, fornecer um formulário dedicado que ajude os usuários a compreender seus direitos e que os oriente a realizar este tipo de solicitações.

Atalhos: ver caso de uso 1 para definição (p. 22) (por exemplo, *fornecer um link para exclusão de conta na conta do usuário*)**.**

Palavras coerentes: ver caso de uso 1 para definição (p.

22). **Fornecer definições**: ver caso de uso 1 para definição

(p. 22). **Uso de exemplos: ver caso de** uso 1 para definição

(p. 22).

Navegação pegajosa: ver caso de uso 2a para definição (p. 28).

Conseqüências Explicativas: ver caso de uso 2c para definição

(p. 32)**. Consistência do dispositivo cruzado: ver caso de** uso 3a

3.5 Tanto tempo e adeus: deixar uma conta na mídia social

Usar o caso 5: pausar a conta/errogativa de todos os dados pessoais

a. Descrição do contexto e disposições legais relevantes

158. O fim do ciclo de vida de uma conta descreve a situação quando os usuários decidem deixar a rede social. Nesta situação, os usuários geralmente decidem deixar a plataforma de mídia social permanentemente. Entretanto, muitas vezes há também a opção de desativar a conta apenas temporariamente e interromper o serviço. As implicações legais de ambas as decisões são diferentes e são descritas abaixo.

i. Apagamento permanente da conta

159. A decisão de abandonar permanentemente a plataforma de mídia social é acompanhada pelo direito de apagamento no Artigo 17 (1) (a) GDPR. Neste contexto, a palavra "apagamento" é usada com mais freqüência do que apagamento.

160. A palavra "apagamento" não está legalmente definida no Artigo 17 GDPR e é mencionada apenas como uma forma de processamento no Artigo 4 (2) GDPR. O apagamento pode ser geralmente entendido como uma impossibilidade (factual) de perceber as informações sobre um indivíduo previamente incorporado nos dados a serem apagados. Após o apagamento, não deve mais ser possível para ninguém perceber as informações em questão sem esforço desproporcional.

161. A anonimização é outra forma de remover permanentemente a relação com uma pessoa. Em outras palavras, o uso de técnicas de anonimização visa garantir que a pessoa em questão não possa mais ser identificada. A anonimização também significa que os princípios da lei de proteção de dados - tais como o princípio da limitação da finalidade - não são mais aplicáveis (ver o considerando 26, frases 4 e 5).

162. De acordo com o artigo 12 (2) da GDPR, o controlador deve facilitar o exercício dos direitos do sujeito dos dados nos termos dos artigos 15 a 22. De acordo com esta exigência, nenhum obstáculo substantivo ou formal pode ser criado na afirmação dos direitos da pessoa em causa. Portanto, se o exercício do direito de apagamento for dificultado sem motivo real, isto constitui uma violação da GDPR. Embora exista uma razão válida para os provedores de mídia social explicarem objetivamente as conseqüências, tais como a eliminação de todos os dados pessoais, e pedirem aos sujeitos dos dados que confirmem esta escolha,[73] também devem ser evitados obstáculos desnecessários neste caso de uso. A partir disto, por exemplo, que qualquer período de carência entre os pedidos de exclusão de conta dos usuários e a exclusão real da conta precisa ser proporcional. Assim, tal tempo pode não ser excessivo, levando em conta as razões técnicas necessárias para atrasos na eliminação imediata, bem como um tempo curto para a (re)consideração dos usuários sobre a eliminação de sua conta uma vez que eles tenham acionado o processo de eliminação da conta. Embora o livre arbítrio dos usuários para mudar de idéia precise ser respeitado, os provedores de mídia social podem não tentar desencadear tal mudança de idéia incitando os usuários a voltar, o que também constituiria um impedimento ao direito dos usuários à exclusão. Durante o período de carência, o processo de exclusão poderia ser interrompido em alguns casos, por exemplo, quando o usuário faz o login novamente. Se a exclusão não puder ser completada, o usuário deve ser informado e instruído sobre como completar a exclusão.

163. A decisão de deixar a plataforma da mídia social desencadeia as conseqüências do apagamento, como indicado no Artigo 17 (1) GDPR. Se um envolvido solicitar a exclusão da respectiva conta, o controlador de uma plataforma de mídia social precisa excluir os dados. Entretanto, alguns dados podem permanecer na plataforma de mídia social por um certo período de tempo se o Artigo 17 (3)

GDPR for aplicável. As exceções enumeradas no artigo 17 (3) da GDPR devem ser interpretadas de forma restrita e só se aplicam nos casos explicitamente mencionados nesta parte da disposição. Qualquer exceção em que um responsável pelo tratamento se baseia nos termos do Artigo 17 (3) GDPR e a respectiva retenção de dados precisa ser justificada pelo responsável pelo tratamento, por exemplo, que a legislação nacional exige que o responsável pelo tratamento armazene informações relacionadas à pessoa em questão por razões imperiosas de interesse público, por

[73] Ao contrário dos outros direitos do sujeito dos dados, ver parágrafo. 154 acima.

exercer o direito fundamental de liberdade de expressão e informação ou por razões fiscais. Escusado será dizer que tais dados restantes só devem ser armazenados internamente pelo Provedor de Mídia Social e não devem ser visíveis publicamente para outros usuários. De forma alguma, entretanto, uma isenção sob o Artigo 17 (3) GDPR permite que o provedor de mídia social mantenha a conta do sujeito dos dados por mais tempo do que o pretendido pelos usuários após seu pedido de exclusão.

164. Independentemente de uma solicitação para apagar a conta, se os usuários retirarem seu consentimento sob o Artigo 7 (3) GDPR, o processamento dos dados fornecidos com base no consentimento sob o Artigo 6 (1) (a) GDPR não poderá mais ter lugar. Neste caso, outras operações de processamento em que o provedor da mídia social se baseia em outras bases legais sob o Artigo 6 (1) GDPR ainda podem, sob certas circunstâncias, ocorrer.

165. Se os usuários pedirem, entretanto, para apagar sua conta, nenhum outro processamento deverá ocorrer, independentemente da base legal subjacente, a menos que uma das exceções enumeradas exaustivamente no Artigo 17 (3) GDPR se aplique. Neste contexto, é importante ter em mente que a retenção é limitada ao armazenamento mínimo acima mencionado.

166. De acordo com o artigo 25 (1) da GDPR, o responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para colocar em prática os princípios de proteção de dados. De acordo com as Diretrizes 04/2019 sobre o Artigo 25 - Proteção de Dados por Projeto e por Padrão, medidas técnicas e organizacionais podem ser entendidas em um sentido amplo como qualquer método ou meio que o responsável pelo tratamento possa empregar no processamento. Ser apropriado significa que as medidas devem ser adequadas para atingir o objetivo pretendido, ou seja, devem implementar os princípios de proteção de dados de forma eficaz. A exigência de adequação está, portanto, estreitamente relacionada com a exigência de eficácia.[74]

[74] Diretrizes 04/2019 sobre Proteção de Dados por Projeto e por Padrão, página 6, para. 8.

ii. Pausando a conta

167. Alternativamente, é oferecida aos usuários a oportunidade de desativar temporariamente sua conta, o que permite aos usuários deixar a mídia social por um período de tempo sem deletar sua conta permanentemente. Neste caso, a conta é temporariamente desativada e o perfil, imagens, comentários e reações serão ocultados até que os usuários reativem sua conta, por exemplo, fazendo o login novamente. A principal diferença para o apagamento é que os dados pessoais permanecem na rede social e a conta pode ser reativada pelos usuários sem um novo registro.

168. Os usuários que iniciam o processo de exclusão de sua conta podem descobrir que a opção de pausar a conta em vez disso é pré-selecionada. Embora possa ser útil para os usuários que não gostariam de excluir permanentemente sua conta ainda para ser oferecida uma opção de pausa, os provedores de mídia social podem não impor tais períodos de pausa aos usuários, especialmente através da pré-seleção. Ao oferecer a possibilidade de desativação, o provedor de mídia social aumenta as expectativas razoáveis dos usuários de que seus dados pessoais não serão processados da mesma forma que durante o uso ativo da conta e que o provedor de mídia social reduz o processamento de dados pessoais a um nível estritamente necessário durante este período. Os usuários podem esperar que seus dados não sejam ou não sejam totalmente processados para fins específicos, por exemplo, melhorando seu perfil com visitas a websites de terceiros que utilizam ferramentas apropriadas de direcionamento ou rastreamento. Além de informar os usuários de forma transparente sobre as conseqüências da pausa de sua conta, qualquer processamento de dados que ocorra durante esta pausa precisa contar com uma base legal válida.

169. Em relação ao processamento de dados com base no consentimento de acordo com o Artigo 6 (1) (a) GDPR, o provedor da mídia social deve levar em conta que os usuários esperam que o consentimento que dão durante o registro ou posteriormente só cubra o processamento de dados durante seu uso ativo da conta. A EDPB reconhece que a duração do consentimento depende do contexto, do escopo do consentimento inicial e das expectativas do sujeito dos dados.[75] Embora não haja um limite de tempo específico na GDPR para a duração do consentimento, a validade dependerá do contexto, do escopo do consentimento original e das expectativas do sujeito dos dados.[76] Se as operações de processamento mudarem ou evoluírem consideravelmente, então o consentimento original não será mais válido.[77] A EDPB recomenda como melhor prática que o consentimento deve ser atualizado em intervalos apropriados.[78] O fornecimento de todas as informações novamente ajuda a garantir que os sujeitos dos dados permaneçam bem informados sobre como seus dados estão sendo utilizados e como exercer seus direitos.[79] Se este for o caso, o consentimento precisa ser obtido novamente.[80] e todos os requisitos correspondentes devem ser cumpridos.

170. As expectativas razoáveis do sujeito dos dados também devem ser levadas em consideração quando o artigo 6 (1) (f) GDPR for aplicável (ver o considerando 47). Em particular, é necessário considerar se a pessoa em questão pode razoavelmente esperar, no momento e no contexto da coleta dos dados pessoais, que o processamento para esse fim possa estar ocorrendo. Entretanto, os usuários esperam razoavelmente que somente o processamento de dados necessário ocorra durante o momento da desativação. Além disso, o fornecedor da mídia social só pode confiar no interesse legítimo se todas as etapas do teste de interesse legítimo, incluindo o exercício de equilíbrio, forem cumpridas. Qualquer interesse superior ou direitos e liberdades fundamentais da pessoa em questão deve ser avaliado caso a caso.

[75] Diretrizes 5/2020 sobre consentimento, para 110.

[76] Diretrizes 5/2020 sobre consentimento, para 110.
[77] Diretrizes 5/2020 sobre consentimento, para 110.
[78] Diretrizes 5/2020 sobre consentimento, para 111.
[79] Diretrizes 5/2020 sobre consentimento, para 111.
[80] Ver Diretrizes 5/2020 sobre consentimento, para 110.

171. Como as obrigações contratuais também são suspensas em grande parte durante a desativação, as operações de processamento de dados só são necessárias até certo ponto sob o Artigo 6 (1) (b) GDPR. Somente o armazenamento dos dados dos usuários até a decisão final sobre a reativação ou apagamento pode ser considerado necessário.

172. Tendo em vista que todo o processamento de dados anteriores tinha como objetivo uma conta ativa, informações adicionais sobre o processamento durante a desativação devem ser fornecidas se não estiverem incluídas nas informações gerais sob os artigos 13, 14 GDPR. Isto decorre dos princípios de transparência e equidade sob o Artigo 5 (1) (a) GDPR e limitação de propósito do Artigo 5 (1) (b) GDPR. O processamento dos dados após a desativação deve ser acompanhado de informações suficientes da pessoa em questão. Portanto, o fornecedor da mídia social deve informar amplamente os usuários sobre o processamento real e seus objetivos durante a pausa e, se necessário, obter novo consentimento.

b. Padrões de design enganosos

i. Padrões baseados no conteúdo

Sobrecarga - Labirinto de Privacidade (Anexo I lista de verificação 4.1.2)

173. Neste caso de uso, o padrão de design enganoso O ***labirinto de privacidade*** ocorre quando os usuários são enterrados sob uma massa de informações, espalhadas por vários lugares, para evitar que eles apaguem sua conta, como mostra o exemplo abaixo. Embora algumas informações adicionais antes desta etapa sejam bastante desejáveis, tais como a indicação de que os usuários têm acesso aos seus dados antes da exclusão, as informações gerais não relacionadas não são mais cruciais. Os usuários não devem ser desnecessariamente atrasados nesta etapa.

> **Exemplo 52:** Os usuários estão procurando o direito de apagamento. Eles têm que chamar as configurações da conta, abrir um submenu chamado "privacidade" e têm que percorrer todo o caminho para baixo para encontrar um link para apagar a conta.

Agitação - Direção Emocional (Anexo I lista de verificação 4.3.1)

> **Exemplo 53:** No primeiro nível de informação, a informação é dada aos usuários destacando apenas as consequências negativas e desencorajadoras da exclusão de suas contas (por exemplo: *"você perderá tudo para sempre"* ou *"seus amigos esquecerão de você"*).

174. Enquanto o pesar pela rescisão da relação contratual parece socialmente adequado e, portanto, difícil de capturar em termos legais, uma descrição abrangente das conseqüências supostamente negativas causadas pelos usuários ao apagar sua conta constitui um impedimento contra sua decisão se feita como no exemplo acima que joga com o medo de perder (FOMO), fazendo com que a escolha de apagar sua conta pareça particularmente punitiva. Tal ***direção emocional***, ameaçando os usuários de que serão deixados em paz se apagarem sua conta, constitui uma violação da obrigação de facilitar o exercício dos direitos da pessoa em questão nos termos do Artigo 12 (2) GDPR, bem como do princípio de justiça nos termos do Artigo 5 (1) (a) GDPR.

Esquerda na escuridão - texto ou informações ambíguas (Anexo I lista de verificação 4.6.3)

175. No contexto da eliminação de uma conta de mídia social, os usuários também podem ser confrontados com o padrão de design enganoso, com ***palavras ou informações ambíguas***, como mostrado no

exemplo a seguir.

Exemplo 54: Quando os usuários excluem sua conta, eles não são informados sobre o tempo em que seus dados serão mantidos, uma vez que a conta é excluída. Pior ainda, em nenhum

Os usuários do processo são aconselhados sobre o fato de que "*alguns dos dados pessoais*" podem ser armazenados mesmo após a exclusão de uma conta. Eles precisam procurar as informações por si mesmos, através das diferentes fontes de informação disponíveis.

Exemplo 55: Os usuários só podem excluir sua conta através de links chamados *"Veja você"* ou *"Desativar"* disponível em sua conta.

176. Nestes exemplos, o texto utilizado para os links não transmite claramente o fato de que os usuários serão redirecionados para o processo de exclusão de conta. Em vez disso, os usuários provavelmente pensarão em outras funcionalidades, tais como o log off até o próximo uso, ou a desativação de sua conta. Como tal, isto poderia ser interpretado como uma violação do Artigo 12 (2) GDPR, que estabelece que os controladores de dados devem facilitar o exercício dos direitos das pessoas em questão. Ao criar confusão sobre as expectativas dos usuários associadas ao link, a plataforma de mídia social não facilita totalmente o exercício do direito de apagamento. O uso de tais palavras equivocadas em outro contexto poderia infringir as disposições da GDPR, como o Artigo 7 GDPR e, por extensão, o Artigo 17 (1) (b) GDPR.

ii. Padrões baseados em interfaces

Pular - Aconchego enganoso (Anexo I lista de verificação 4.2.1)

Exemplo 56: No processo de exclusão de sua conta, os usuários têm duas opções à sua disposição: excluir sua conta ou pausá-la. Por padrão, a opção de pausar é selecionada.

177. A primeira opção de excluir a conta resulta na exclusão de todos os dados pessoais dos usuários, o que significa que a plataforma de mídia social não está mais na posse desses dados, exceto para os dados sob a exceção temporária do Artigo 17 (3) GDPR. Em contraste, com a segunda opção de pausar a conta, todos os dados pessoais são mantidos e potencialmente processados pelo provedor da mídia social. Isto necessariamente representa mais riscos para o envolvido, por exemplo, se ocorrer uma violação de dados e os dados ainda armazenados pelo provedor de mídia social forem acessados, duplicados, transferidos ou processados de outra forma. A seleção padrão da opção de pausa é susceptível de incitar os usuários a selecioná-la em vez de apagar sua conta como inicialmente pretendido. Portanto, a prática descrita neste exemplo pode ser considerada como uma violação do Artigo 12 (2) GDPR, uma vez que não facilita, neste caso, o exercício do direito de apagamento, e até mesmo tenta coagir os usuários a não exercê-lo.

Skipping - Veja ali (Anexo I lista de verificação 4.2.2)

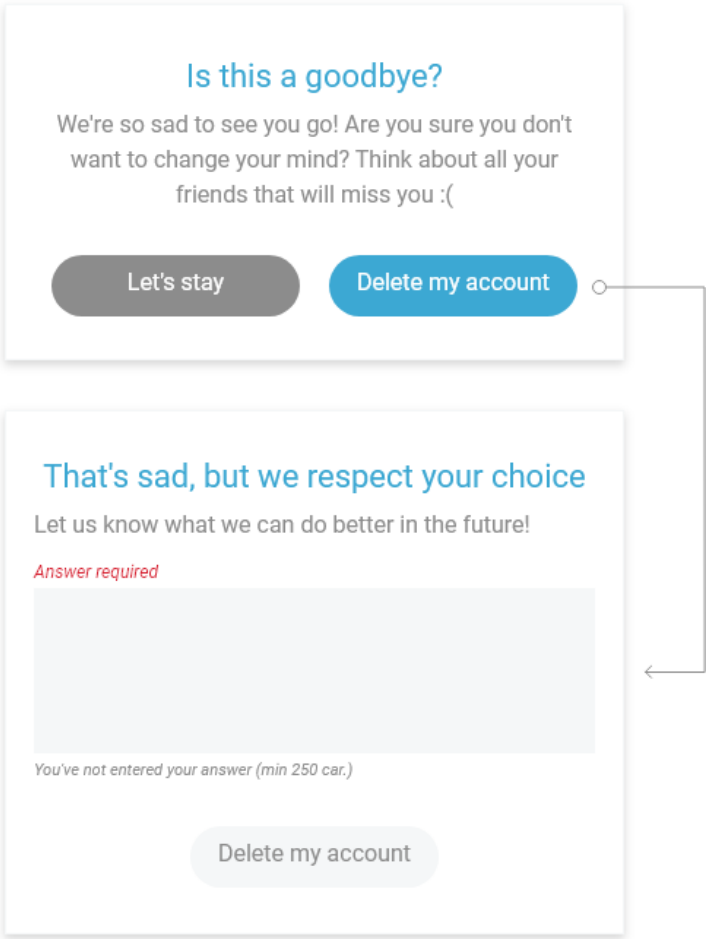
178. Fornecer aos usuários um meio de baixar seus dados quando eles indicam sua vontade de excluir sua conta pode ser uma opção relevante a oferecer. De fato, uma vez que sua conta for excluída, seus dados pessoais serão apagados após um certo período de tempo. Isto significa que, se eles não obtiverem uma cópia de seus dados pessoais, eles os perderão completamente. Entretanto, a apresentação desta opção pode constituir um padrão de design enganoso, como mostrado no exemplo a seguir.

Exemplo 57: Após clicar em "Apagar minha conta", é apresentada aos usuários a opção de baixar seus dados, implementada como o direito à portabilidade, antes de apagar a conta. Ao clicar para fazer o download de suas informações, os usuários são redirecionados em uma página de informações para download. Entretanto, uma vez que os usuários tenham escolhido o que e como baixar seus dados, eles não são redirecionados para o processo de

179. No exemplo acima, poderia ser considerado que a forma como a opção de download é implementada não facilita o exercício do direito de apagamento associado à exclusão da conta. De fato, uma vez que os usuários tenham feito o download de seus dados, eles não são levados de volta ao processo de exclusão. Para voltar a ele, eles terão que clicar várias vezes. Impedir de tal forma o exercício de um direito infringe o Artigo 12 (2) GDPR. Além disso, proporcionar um meio de alcançar facilmente o processo de eliminação após o download de seus dados é um recurso simples de ser implementado. A esse respeito, pode-se considerar que a obrigação de implementar medidas técnicas e organizacionais apropriadas no Artigo 25 (1) GDPR não é respeitada, pois os usuários não são capazes de continuar a exercer seus direitos de forma eficaz.

Obstrução - Mais longa do que o necessário (Anexo I lista de verificação 4.4.2)

180. Conforme detalhado no caso 4, qualquer medida irrelevante acrescentada ao exercício de um direito pode violar as disposições do GDPR, em particular o artigo 12 (2). Isto se aplica ao momento em que os usuários pretendem apagar sua conta, pois isso interferiria no direito de apagamento associado a tal pedido.



Exemplo 58: Neste exemplo, os usuários vêem primeiro uma caixa de confirmação para apagar sua conta após terem clicado no link ou botão correspondente em sua conta. Embora haja alguma ***Direção Emocional*** nesta caixa, esta etapa pode ser vista como uma medida de segurança para que os usuários não apaguem sua conta após um clique errado em sua conta. Entretanto, quando os usuários clicam no botão "Deletar minha conta", são

para descrever textualmente o motivo pelo qual eles querem deixar a conta. Desde que não tenham inserido algo na caixa, não podem apagar sua conta, pois o botão associado à ação está inativo e cinzento. Esta prática faz com que o apagamento de uma conta ***seja mais longo do que o necessário***, especialmente porque pedir aos usuários que produzam um texto descrevendo o motivo pelo qual eles querem sair de uma conta requer esforço e tempo extras e não deve ser obrigatório apagar a conta de alguém.

181. Como observado anteriormente, ao exercer um direito, os usuários não devem ter que responder perguntas não relacionadas com o exercício do próprio direito. Ter que justificar sua escolha ou explicar como a plataforma de mídia social deve melhorar não se enquadra nessa categoria. No exemplo ilustrado, esta questão é agravada, pois os sujeitos dos dados têm que escrever uma resposta em vez de selecionar uma proposta pré-fabricada em uma lista, o que é ainda mais oneroso para eles, uma vez que requer a criação completa da resposta. Tal mecanismo poderia excluir alguns usuários do exercício total de seu direito se eles não se sentissem confortáveis o suficiente para escrever uma resposta.

182. Entretanto, isto não significa que uma lista de respostas pré-fabricadas seja um passo aceitável a ser adicionado ao processo de exclusão da conta. Isto é especialmente verdadeiro se estas respostas estiverem associadas a outras etapas e ações impostas aos usuários, como mostra o exemplo abaixo*.*

Exemplo 59: O provedor de mídia social torna obrigatório que os usuários respondam a uma pergunta sobre suas razões para querer apagar sua conta, através de uma seleção de respostas a partir de um menu suspenso. Parece aos usuários que responder a esta pergunta (aparentemente) lhes permite realizar a ação que desejam, ou seja, apagar a conta. Uma vez selecionada uma resposta, aparece uma janela pop-up, mostrando aos usuários uma forma de resolver o problema indicado em sua resposta.

183. Além de tornar o apagamento da conta particularmente demorado, um mecanismo de ***"Look Over There"*** visa desviar os usuários da eliminação de sua conta, fornecendo uma solução para sua motivação ao deixar para trás a plataforma de mídia social. Isto dificulta o exercício do direito de apagar e, por extensão, desencoraja os indivíduos a exercerem seu direito.

Fickle - Descontextualização (Anexo I lista de verificação 4.5.2)

184. Finalmente, o padrão de design enganoso ***da Decontextualização*** também pode ser encontrado quando os usuários desejam excluir sua conta.

Exemplo 60: Na plataforma de mídia social XY, o link para desativar ou excluir a conta é encontrado na guia "*Seus dados XY".*

185. Em geral, os termos usados para denominar uma página ou seção da plataforma de mídia social dedicada a questões de proteção de dados devem refletir claramente o tipo de informação ou controle ali incluído. É improvável que usuários médios associem ações para apagar ou desativar sua conta ao gerenciamento de dados. No exemplo anterior, os usuários não esperariam a funcionalidade de excluir sua conta em uma página chamada "Suas Informações XY" que alude a ver e potencialmente rever as informações de uma pessoa. Ao invés disso, eles procurariam uma página "Geral" ou uma página "Excluir minha conta". Portanto, do ponto de vista dos usuários, as opções

são colocadas em um cenário que está fora do contexto e não corresponde às expectativas do usuário.

Exemplo 61: A aba real para apagar uma conta é encontrada na seção "*apagar uma função de sua conta*".

186. Neste exemplo, os usuários poderiam entender erroneamente o título da seção como o mero lugar onde ajustar funções individuais. Portanto, os usuários não esperariam que a opção de excluir a conta inteira estivesse lá. Isso torna difícil para os usuários encontrar o link correto para apagar a conta inteira.

187. O padrão de design enganoso ***descontextualizante***, como ilustrado nos dois exemplos acima, poderia ser considerado uma violação do Artigo 12 (2) GDPR, uma vez que os usuários teriam dificuldades para encontrar o lugar certo para exercer seu direito de apagamento.

c. Melhores Práticas

Palavras coerentes: ver caso de uso 1 para definição

(p.22). **Fornecer definições**: ver caso de uso 1 para

definição (p.22). **Uso de exemplos: ver caso de** uso 1 para

definição (p.22).

Explicação das conseqüências: ver caso de uso 2c para definição (p.32)**.**

Para o Conselho Europeu de Proteção de

Dados O Presidente

(Andrea Jelinek)

4 ANEXO I: LISTA DE CATEGORIAS E TIPOS DE PADRÕES DE DESIGN ENGANOSOS

A lista a seguir fornece uma visão geral das categorias de padrões de design enganosos e os tipos de padrões de design enganosos dentro de cada categoria. Ela também lista as disposições da GDPR mais preocupadas com os tipos de padrões de design enganosos. Os leitores devem ter em mente que, como mencionado acima, o princípio de processamento justo estabelecido no Artigo 5 (1) (a) GDPR é um ponto de partida para uma avaliação da existência de padrões de design enganosos. Ela tem uma função de guarda-chuva e todos os padrões de design enganosos não o cumpririam, independentemente do cumprimento de outros princípios de proteção de dados.[81]

Para cada padrão, a lista também contém o número de exemplos e o caso de uso correspondente (UC) para ajudar os leitores a encontrá-los rapidamente.

É importante notar que esta lista não é exaustiva e que padrões de design enganosos também podem ocorrer em casos de uso que não contenham um exemplo para este tipo de padrão de design enganoso no texto das Diretrizes.

4.1 Sobrecarga

Enterrar os usuários sob uma massa de solicitações, informações, opções ou possibilidades, a fim de dissuadi-los de ir mais longe e fazê-los manter ou aceitar certas práticas de dados.

4.1.1 Alerta contínuo[82]

Pressionar os usuários a fornecerem mais dados pessoais do que os necessários para a finalidade de processamento ou para concordar com outro uso de seus dados, solicitando repetidamente aos usuários que forneçam dados ou que consintam em um novo propósito de processamento. Tais solicitações repetitivas podem acontecer através de um ou vários dispositivos. É provável que os usuários acabem cedendo, cansados de ter que recusar o pedido cada vez que utilizam a plataforma, o que os perturba em seu uso.

Disposições preocupantes sobre o GDPR:

- *Limitação de propósito: Artigo 5 (1) (b);*
- *Livre consentimento: Artigo 7* em conjunto com o artigo 4 (11);
- *Consentimento específico: Artigo 7 (2).*

Exemplos: UC 1 exemplos 1, 2; UC 3a exemplo 34 (ilustração).

4.1.2 Labirinto de privacidade

Quando os usuários desejam obter certas informações ou usar um controle específico ou exercer um direito sobre os dados, é particularmente difícil para eles encontrá-lo, pois têm que navegar por muitas páginas a fim de obter as informações ou controle relevantes, sem ter uma visão geral abrangente e exaustiva disponível. É provável que os usuários desistam ou percam as informações ou o controle relevantes.

Disposições preocupantes sobre o GDPR:

[81] Ver acima, para. 9 destas Diretrizes.
[82] Este padrão está intimamente relacionado a um tipo de padrão chamado "Nagging", encontrado na literatura acadêmica.

- *Princípio da transparência*: *Artigo 5 (1) (a) e informação transparente: Artigo 12 (1);*
- *Princípio de justiça: Artigo 5 (1) (a);*
- *Informações de fácil acesso*: Artigo 12 (1);
- *Fácil acesso aos direitos*: Artigo 12 (2);
- *Consentimento informado*: Artigo 7 em conjunto com o artigo 4 (11).

Exemplos: UC 2a exemplo 17; UC 3a exemplo 33; UC 3b exemplo 37; UC 4 exemplos 47 (ilustração) e 48 (ilustração); UC 5 exemplo 51.

4.1.3 Demasiadas opções

Proporcionar aos usuários (também) muitas opções para escolher. A quantidade de escolhas deixa os usuários incapazes de fazer qualquer escolha ou fazê-los ignorar algumas configurações, especialmente se a informação não estiver disponível. Isso pode levá-los a finalmente desistir ou perder as configurações de suas preferências ou direitos de proteção de dados.

Disposições preocupantes sobre o GDPR:

- *Princípios de transparência e justiça:* Artigo 5 (1) a;
- *Informação transparente*: Artigo 12 (1).

Exemplo: UC 3b exemplo 35.

4.2 Saltando

Projetar a interface ou jornada do usuário de tal forma que os usuários esqueçam ou não pensem em todos ou alguns dos aspectos da proteção de dados.

4.2.1 Aconchego enganoso

Por padrão, as características e opções mais invasivas de dados são ativadas. Confiando no efeito padrão, que impele os indivíduos a manter uma opção pré-selecionada, é improvável que os usuários mudem isso, mesmo que seja dada a possibilidade.

Disposições preocupantes sobre o GDPR:

- *Proteção de dados por projeto e por padrão*: Artigo 25 (1);
- *Consentimento:* Artigos 4 (11) e 6 (prática ilegal para ativar um processamento baseado no consentimento por padrão).

Exemplos: UC 1 exemplo 9; UC 3b exemplos 39 e 40 (ilustração); UC 5 exemplo 55.

4.2.2 Olhe para lá

Uma ação ou informação relacionada à proteção de dados é colocada em concorrência com outro elemento que pode ou não estar relacionado à proteção de dados. Quando os usuários escolhem esta opção de distração, é provável que eles esqueçam a outra, mesmo que fosse sua intenção principal.

Disposições preocupantes sobre o GDPR:

- *Princípios de transparência e justiça:* Artigo 5 (1) a;
- *Informação transparente*: Artigo 12 (1);
- *Exercício dos direitos:* Artigo 12 (2).

Exemplos: UC 2c exemplo 25; UC 3a exemplo 29; UC 5 exemplos 56 e 58.

4.3 Agitando

Afetar a escolha que os usuários fariam ao apelar para suas emoções ou ao usar empurrões visuais.

4.3.1 Direção Emocional[83]

Usando palavras ou elementos visuais (tais como estilo, cores, imagens ou outros) de uma forma que confira a informação aos usuários em uma perspectiva altamente positiva, fazendo com que os usuários se sintam bem, seguros ou recompensados, ou em uma perspectiva altamente negativa, fazendo com que os usuários se sintam assustados, culpados ou punidos. Influenciar o estado emocional dos usuários de tal forma provavelmente os levará a tomar uma ação que funcione contra seus interesses de proteção de dados.

Disposições preocupantes sobre o GDPR:

- *Princípios de transparência e justiça:* Artigo 5 (1) a;
- *Informação transparente*: Artigo 12 (1);
- *Exercício dos direitos:* Artigo12 (2);
- *Consentimento da criança:* Artigo 8;
- *Consentimento informado*: Artigo 7 em conjunto com o artigo 4 (11);

Exemplos: UC1 exemplos 4, 5, 6; UC 5 exemplo 52.

4.3.2 Escondido à vista de todos

Usar um estilo ou técnica visual para controles de informação ou proteção de dados que impele os usuários para opções menos restritivas e, portanto, mais invasivas.

Disposições preocupantes sobre o GDPR:

- *Princípio de justiça*: Artigo 5 (1) a;
- *Livre consentimento:* Artigo 7 em conjunto com o artigo 4(11);
- *Informações claras*: Artigo 12 (1);
- *Exercício dos direitos:* Artigo12 (2)

Exemplos: UC1 exemplo 8, UC 3a exemplo 34 (ilustração); UC 3b exemplo 40 (ilustração); UC 4 exemplo 48.

[83] Este padrão está intimamente relacionado a um tipo de padrão chamado "*Brincando com Emoções*" encontrado, entre outros, em relatórios de organizações intergovernamentais como Comissão Européia, Direção Geral de Justiça e Consumidores, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al, *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : relatório final*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030 e OECD (2022), "Dark commercial patterns", *Documents de travail de l'OCDE sur l'économie numérique*, n° 336, Éditions OCDE, Paris, https://doi.org/10.1787/44f5e846-en.

4.4 Obstrução[84]

Impedir ou bloquear os usuários em seu processo de obtenção de informações ou gerenciamento de seus dados, tornando a ação difícil ou impossível de ser realizada.

4.4.1 Beco sem saída

Enquanto os usuários estão procurando informações ou um controle, eles acabam não encontrando como um link de redirecionamento, ou não está funcionando ou não está disponível de todo. Os usuários ficam impossibilitados de realizar essa tarefa.

Disposições preocupantes sobre o GDPR:

- *Informações de fácil acesso*: Artigo 12 (1);
- *Exercício dos direitos*: Artigo 12 (2);
- *Proteção de dados por projeto e por padrão*: Artigo 25 (1).

Exemplos: UC1 exemplos 10, 11; UC 2a exemplo 18; UC 3a exemplos 30, 31; UC 4 exemplo 43.

4.4.2 Mais tempo do que o necessário

Quando os usuários tentam ativar um controle relacionado à proteção de dados, a viagem do usuário é feita de uma forma que requer mais passos dos usuários, do que o número de passos necessários para a ativação de opções invasivas de dados. Isto provavelmente os desencoraja de ativar tal controle.

Disposições preocupantes sobre o GDPR:

- *Informações de fácil acesso*: Artigo 12 (1);
- *Exercício dos direitos*: Artigo 12 (2);
- *Direito de objeção*: Artigo 21 (1);
- *Retirada autorizada*: Artigo 7 (3);
- *Proteção de dados por projeto (e por padrão)*: Artigo 25 (1).

Exemplos: UC 1 exemplo 7; UC 3a exemplo 32; UC 4 exemplo 50; UC 5 exemplos 57 (ilustração) e 58.

4.4.3 Ação enganosa

Uma discrepância entre informações e ações disponíveis para os usuários os impele a fazer algo que eles não pretendem fazer. A diferença entre o que os usuários esperam e o que eles recebem provavelmente os desencoraja de ir mais longe.

Disposições preocupantes sobre o GDPR:

- *Informação transparente*: Artigo 12 (1);
- *Equidade de processamento*: Artigo 5 (1) (a).

[84] Esta categoria está intimamente relacionada à estratégia chamada "*Obstrução*" definida e descrita em Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph e Toombs Austin L. 2018. O Lado Escuro (Padrões) do Projeto

UX. Em Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canadá) (CHI '18). ACM, Nova York, NY, EUA, Artigo 534, 14 páginas. https://doi.org/10.1145/3173574.3174108.

- *Consentimento informado*: Artigo 7 (2) em conjunto com o artigo 4 (11).

Exemplos: UC 1 exemplo 3; UC 3a exemplo 28.

4.5 Fickle

O design da interface é instável e inconsistente, tornando difícil para os usuários descobrir a natureza do processamento, fazer uma escolha adequada em relação aos seus dados e encontrar onde estão os diferentes controles.

4.5.1 Falta de hierarquia

As informações relacionadas à proteção de dados carecem de hierarquia, fazendo com que as informações apareçam várias vezes e sejam apresentadas de várias maneiras. É provável que os usuários fiquem confusos com esta redundância e fiquem impossibilitados de entender completamente como seus dados são processados e como exercer controle sobre eles.

Disposições preocupantes sobre o GDPR:

- *Informações de fácil acesso*: Artigo 12 (1);
- *Exercício dos direitos: Artigo 12 (2).*

Exemplos: UC 2a exemplos 13 e 14.

4.5.2 Descontextualizando

Uma informação ou controle de proteção de dados está localizado em uma página que está fora do contexto. É improvável que os usuários encontrem a informação ou o controle, pois não seria intuitivo procurá-lo nesta página específica.

Disposições preocupantes sobre o GDPR:

- *Informações de fácil acesso*: Artigo 12 (1);
- *Informação transparente*: Artigo 12 (1);
- *Exercício dos direitos: Artigo 12 (2).*

Exemplos: UC 3b exemplos 41, 42; UC 5 exemplos 59 e 60.

4.5.3 Interface incoerente

Uma interface não é consistente entre diferentes contextos (por exemplo, um menu relacionado à proteção de dados não exibe os mesmos itens no celular e no desktop) ou com as expectativas dos usuários (por exemplo, uma opção cuja localização tenha sido trocada com a de outra opção). Estas diferenças podem levar os usuários a não encontrar o controle ou a informação desejada ou a interagir com um elemento da interface fora dos hábitos, embora esta interação leve a fazer uma escolha de proteção de dados que os usuários não desejam.

Disposições preocupantes sobre o GDPR:

- *Informações de fácil acesso*: Artigo 12 (1);

- *Exercício dos direitos: Artigo 12 (2).*

Exemplos: UC 3b exemplo 39; UC 4 exemplo 50.

4.5.4 Descontinuidade do idioma

As informações relacionadas à proteção de dados não são fornecidas no(s) idioma(s) oficial(is) do país onde os usuários vivem, enquanto que o serviço é. Se os usuários não dominarem o idioma no qual as informações sobre proteção de dados são fornecidas, eles não poderão lê-las facilmente e, portanto, provavelmente não estarão cientes de como os dados são processados.

Disposições preocupantes sobre o GDPR:

- *Equidade de processamento*: Artigo 5 (1) (a);
- *Informações inteligíveis*: Artigo 12 (1), Artigo 13 e Artigo 14;
- *Uso de linguagem clara e clara para a informação*: Artigo 12 (1), Artigo 13 e Artigo 14.

Exemplos: UC 2a exemplo 16; UC 3a exemplos 26 (ilustração) e 27; UC 4 exemplo 44.

4.6 Deixado no escuro

A interface é projetada de forma a ocultar informações ou controles relacionados à proteção de dados ou para deixar os usuários inseguros sobre como os dados são processados e que tipo de controles eles podem ter sobre eles.

4.6.1 Informações conflitantes

Fornecendo informações aos usuários que entram em conflito entre si de alguma forma. É provável que os usuários fiquem inseguros sobre o que devem fazer e sobre as conseqüências de suas ações, portanto, é provável que não tomem nenhuma e apenas mantenham as configurações padrão.

Disposições preocupantes sobre o GDPR:

- *Equidade de processamento*: Artigo 5 (1) (a);
- *Informação transparente*: Artigo 12 (1);
- *Consentimento informado*: Artigo 7 (2) em conjunto com o artigo 4 (11).

Exemplos: UC 2a exemplo 12; UC 2c exemplo 20; UC 3b exemplo 36.

4.6.2 Escritos ou informações ambíguos

Usando termos ambíguos e vagos ao dar informações aos usuários. É provável que não tenham certeza de como os dados serão processados ou de como exercer controle sobre seus dados pessoais.

Disposições preocupantes sobre o GDPR:

- *Equidade de processamento*: Artigo 5 (1) (a);
- *Informação transparente*: Artigo 12 (1);
- *Uso de linguagem clara e clara para a informação*: Artigo 12 (1);

- *Consentimento informado*: Artigo 7 (2) em conjunto com o artigo 4 (11);
- *Informações incompletas*: Artigo 13
- *Disposições específicas dependendo do caso particular de uso, por exemplo,* o artigo 34 *para a UC 2c*.

Exemplos: UC 2a exemplo 15; UC 2c exemplos 21, 22, 23, 24; UC 4 exemplo 45; UC 5 exemplos 53 e 54.


LIFECYCLE
DECEPTIVE DESIGN OVERVIEW
GDPR PROVISIONS
All deceptive design go against the fairness principle
UC 1. Creating an account
UC2. Getting informed
UC3. Staying protected
UC4. Exercising one's right
UC5. Closing / Pausing the account
Purpose limitation
Data protection by design and default
Transparency/Information
Consent
Exercise of the rights
OVERLOADING
Continuous Prompting
Privacy Maze
Too Many Options
SKIPPING
Deceptive Snugness
Look Over There
STIRRING
Emotional Steering
Hidden in Plain Sight
OBSTRUCTING
Dead End
Longer Than Necessary
Misleading Action
FICKLE
Lacking Hierarchy
Decontextualising
Inconsistent Interface
Language Discontinuity
LEFT IN THE DARK
Conflicting Information
Ambiguous Wording or Information

5 ANEXO II: MELHORES PRÁTICAS

A lista a seguir fornece uma visão geral das melhores práticas descritas nas Diretrizes no final de cada caso de uso. Estas podem ser usadas para projetar interfaces de usuário que facilitem a implementação efetiva do GDPR. Tais melhores práticas podem oferecer um primeiro passo para uma maneira padronizada de os usuários controlarem efetivamente seus dados e exercerem seus direitos.

Atalhos: Links para informações, ações ou configurações que possam ser de ajuda prática aos usuários para gerenciar seus dados e suas configurações de proteção de dados devem estar disponíveis onde quer que eles sejam confrontados com informações ou experiências relacionadas (por exemplo, *links redirecionando para as partes relevantes da política de privacidade*; por *exemplo na política de privacidade, fornecer para cada link de informação de proteção de dados que redireciona diretamente para as páginas de proteção de dados relacionados na plataforma de mídia social; fornecer aos usuários um link para redefinir sua senha*; *quando os usuários são informados sobre um aspecto do processamento, eles são convidados a definir suas preferências de dados relacionados na página de configuração/dashboard correspondente; fornecer um link para exclusão de conta na conta do usuário*)**.**

Opções a granel: Colocar opções que têm a mesma finalidade de processamento juntas, para que os usuários possam mudá-las mais facilmente, deixando ainda aos usuários a possibilidade de fazer mudanças mais granulares. Se as plataformas de mídia social apresentarem opções em massa, estas não devem conter elementos inesperados ou não relacionados (por exemplo, elementos com finalidades diferentes). Se o processamento exigir consentimento, as opções em massa devem estar de acordo com as Diretrizes da EDPB sobre consentimento, especialmente o parágrafo. 42-44.

Informações de contato: O endereço de contato da empresa para tratar dos pedidos de proteção de dados deve ser claramente indicado na política de privacidade. Deve estar presente em uma seção onde os usuários podem esperar encontrá-lo, como uma seção sobre a identidade do controlador dos dados, uma seção relacionada aos direitos ou uma seção de contato.

Chegar à autoridade supervisora: Declarar a identidade específica da autoridade fiscalizadora e incluir um link para seu website ou para a página específica do website relacionada com a apresentação de uma reclamação. Esta informação deve estar presente em uma seção onde os usuários podem esperar encontrá-la, como uma seção relacionada a direitos.

Visão geral da Política de Privacidade: No início / topo da política de privacidade, inclua um índice (dobrável) com títulos e subtítulos que mostrem as diferentes passagens que a nota de privacidade contém. Os nomes das passagens individuais conduzem claramente os usuários quanto ao conteúdo exato e permitem que eles identifiquem rapidamente e saltem para a seção que estão procurando.

Manchas de mudança e comparação: Quando forem feitas alterações no aviso de privacidade, torne as versões anteriores acessíveis com a data de lançamento e destaque as alterações.

Palavras coerentes: Em todo o site, a mesma formulação e definição é usada para a mesma proteção de dados. A redação usada na política de privacidade deve corresponder à usada no resto da plataforma.

Fornecendo definições: Ao utilizar palavras ou jargões não familiares ou técnicos, fornecer uma

definição em linguagem simples ajudará os usuários a compreender as informações fornecidas a eles. A definição pode ser dada diretamente no texto, quando os usuários pairarem sobre a palavra, bem como ser disponibilizada em um glossário.

Elementos contrastantes de proteção de dados: Fazer com que elementos ou ações relacionadas à proteção de dados sejam visualmente marcantes em uma interface que não é diretamente dedicada ao assunto. Por exemplo, ao postar um

mensagem na plataforma, os controles sobre a associação da geolocalização devem estar diretamente disponíveis e claramente visíveis.

Proteção de dados a bordo: Logo após a criação de uma conta, inclua pontos de proteção de dados dentro da experiência de onboarding do provedor de mídia social para que os usuários descubram e definam suas preferências sem problemas. Por exemplo, isto pode ser feito convidando-os a definir suas preferências de proteção de dados após adicionar seu primeiro amigo ou compartilhar seu primeiro posto.

Uso de exemplos: Além das informações obrigatórias que indicam clara e precisamente o objetivo do processamento, exemplos podem ser usados para ilustrar um processamento de dados específico para torná-lo mais tangível para os usuários.

Navegação pegajosa: Ao consultar uma página relacionada à proteção de dados, o índice pode ser exibido constantemente na tela permitindo aos usuários sempre se situar na página e navegar rapidamente no conteúdo graças aos links de ancoragem.

Voltar ao início: Incluir um botão de retorno ao topo na parte inferior da página ou como um elemento pegajoso na parte inferior da janela para facilitar a navegação dos usuários em uma página.

Notificações: As notificações podem ser usadas para conscientizar os usuários sobre aspectos, mudanças ou riscos relacionados ao processamento de dados pessoais (por exemplo, *quando ocorreu uma violação de dados*). Estas notificações podem ser implementadas de várias maneiras, tais como através de mensagens na caixa de entrada, janelas pop-in, banners fixos no topo da página da web, etc.

Explicando as conseqüências: Quando os usuários querem ativar ou desativar um controle de proteção de dados, ou dar ou retirar seu consentimento, informá-los de forma neutra sobre as conseqüências de tal ação.

Consistência de dispositivos cruzados: Quando a plataforma de mídia social está disponível através de diferentes dispositivos (por exemplo, computador, smartphones, etc.), as configurações e informações relacionadas à proteção de dados devem estar localizadas nos mesmos espaços através das diferentes versões e devem ser acessíveis através da mesma viagem e elementos de interface (menu, ícones, etc.).

Diretório de proteção de dados: Para uma fácil orientação através da seção diferente do menu, forneça aos usuários uma página facilmente acessível de onde todas as ações e informações relacionadas à proteção de dados são acessíveis. Esta página pode ser encontrada no menu principal de navegação do provedor de mídia social, a conta do usuário, através da política de privacidade, etc.

Informação contextual: além de uma política de privacidade exaustiva, traga pequenos pedaços de informação no momento mais apropriado para que o usuário tenha uma informação específica e contínua sobre como seus dados são processados.

URL auto-explicativa: páginas relacionadas a configurações de proteção de dados ou informações devem usar um endereço web que reflita claramente seu conteúdo. Por exemplo, uma página centralizando o controle de proteção de dados poderia ter um URL tal como [social-network.com]/data-settings.

Exercício do formulário de direitos: para facilitar aos usuários o exercício de seus direitos GDPR, fornecer um formulário dedicado que ajude os usuários a compreender seus direitos e que os oriente a realizar este tipo de solicitações.