

Regulação e Economia de Dados

Produto 1

Análises dos documentos *Data Governance Act* e *Data Act* da União Europeia

Outubro de 2024



Cofinanciado pela União Europeia



on the basis of a decision by the German Bundestag



MINISTÉRIO DO DESENVOLVIMENTO INDÚSTRIA, COMÉRCIO E SERVIÇOS



Ficha técnica

Este documento tem o objetivo de apresentar uma análise concisa dos princípios subjacentes e dos elementos centrais do *Data Act* e do *Data Governance Act*, da União Europeia (UE), em relação ao seu impacto potencial em casos de uso comercial de dados em diferentes setores econômicos. Além disso, essa publicação inclui estimativas sobre as oportunidades de negócio para o mercado da UE.

O conteúdo foi desenvolvido pelo Núcleo de Engenharia Organizacional da Universidade Federal do Rio Grande do Sul (NEO-UFRGS), especialmente para o Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC) do Brasil, com apoio do projeto Diálogo Digital Brasil-União Europeia, uma parceria da União Europeia com o Ministério Federal Alemão para Digital e Transporte (BMDV), e implementado pela *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH* como parte dos Diálogos Digitais Internacionais.

Elaboração

NEO-UFRGS (incluindo projeto gráfico, diagramação e revisão)

Prof. Alejandro G. Frank, Dr.

Prof. Néstor F. Ayala, Dr.

Estefanía Scherf, Eng.

Leonardo Bertoletti

Laura Martins

GIZ

Johannes Klingberg

Júlia Rosa

MDIC

Marcos César de Oliveira Pinto

Publicado por

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Brasília, Brasil 2024

É permitida a reprodução parcial ou total desta obra, desde que citada como fonte o projeto Diálogo Digital Brasil-União Europeia e, para outros usos comerciais, duplicação, reprodução ou distribuição de todo ou partes desta publicação, é necessário o consentimento por escrito da *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH*.

As ideias e opiniões expressas nesta publicação são de autoria e responsabilidade de quem as escreveu, não refletindo, necessariamente, a posição da União Europeia, do BMDV, do MDIC ou da GIZ.

Sumário

Ficha técnica.....	1
Sumário Executivo.....	5
1. Introdução.....	8
2. Data Governance Act.....	11
2.1. Conceitos.....	11
2.2. Atores.....	12
2.3. Princípios do <i>Data Governance Act</i>	12
2.3.1. Confiança.....	12
2.3.2. Consentimento.....	13
2.3.3. Interesse público.....	13
2.4. Mecanismos e boas práticas para a partilha de dados.....	14
2.4.1. Reutilização de dados detidos pelo Setor Público.....	14
2.4.2. Intermediação na partilha de dados.....	15
2.4.3. Altruísmo de dados.....	17
2.4.4. Comitê Europeu da Inovação de Dados.....	19
2.4.5. Acesso e transferências internacionais de dados.....	20
3. Data Act.....	22
3.1. Conceitos.....	23
3.2. Atores.....	24
3.3. Princípios do Data Act.....	24
3.3.1. Soberania de dados.....	24
3.3.2. Acesso equitativo a dados.....	24
3.3.3. Transparência e confiança.....	25
3.3.4. Interoperabilidade.....	25
3.3.5. Portabilidade de dados.....	25
3.4. Papel dos atores para o acesso e uso de dados.....	26
3.4.1. Usuários.....	26
3.4.2. Detentores de dados.....	26
3.4.3. Terceiros.....	27
3.4.4. Organismos do setor público.....	28
3.4.5. Prestadores de serviços de tratamento de dados.....	28
3.4.6. Participantes de espaços de dados.....	28

3.4.7.	Implementadores de contratos inteligentes.....	28
3.4.8.	Órgãos de implementação	29
4.	Potenciais desafios das regulamentações.....	31
4.1.	Desafios regulatórios.....	31
4.2.	Desafios comerciais.....	32
4.3.	Desafios estruturais.....	32
4.4.	Desafios de privacidade	33
5.	Benefícios esperados.....	35
6.	Perdas por falta de regulamentações	38
7.	Conclusões.....	40
8.	Referências.....	41

Sumário Executivo

Este relatório analisa o impacto das legislações europeias—o **Data Governance Act (DGA)** e o **Data Act**—no uso comercial de dados em diversos setores econômicos, com o objetivo de identificar oportunidades de negócio e fornecer recomendações para o desenvolvimento de um marco regulatório adequado à economia de dados no Brasil. Como primeiro produto do projeto "**Regulação e Economia de Dados: Comparativo EU-BR**", o estudo busca compreender os princípios fundamentais e os aspectos principais dessas duas regulamentações, assim como o impacto prático esperado na economia de dados da União Europeia.

Data Governance Act

O DGA é um dos pilares essenciais da estratégia europeia para dados, destinado a promover o compartilhamento voluntário e seguro de informações. Ele estabelece diretrizes de mercado que devem ser seguidas por todos os participantes do mercado europeu, independentemente de sua localização, ampliando o alcance das normas da UE além de suas fronteiras. O foco está na criação de um mercado único digital e em espaços de dados comuns que impulsionem uma economia digital eficiente e atrativa.

Principais disposições do DGA:

- **Reutilização de dados não abertos:** Estabelece condições para a reutilização de determinadas categorias de dados não abertos detidos por organismos do setor público, como dados protegidos por propriedade intelectual ou segredos comerciais. Não concede direitos automáticos nem impõe obrigações, mas define uma estrutura para as condições de reutilização desses dados, caso seja permitida.
- **Serviços de intermediação de dados:** Implementa um regime de notificação e supervisão para a prestação desses serviços, garantindo neutralidade e confiabilidade no compartilhamento de dados.
- **Altruísmo de dados:** Cria uma estrutura que incentiva o compartilhamento voluntário e sem recompensa de dados por indivíduos e organizações para fins benéficos à sociedade.
- **Comitê Europeu da Inovação de Dados:** Estabelece um regime para a criação deste comitê, visando promover a inovação e a coordenação no espaço de dados europeu.
- **Fluxo internacional seguro de dados:** Adota medidas para permitir a transferência segura de dados não pessoais para fora da UE, fortalecendo a posição europeia no cenário global de dados.

Data Act

Complementando o DGA, o Data Act fornece clareza jurídica sobre o acesso e o uso de dados pessoais e não pessoais, contribuindo para a formação de um mercado único de dados na UE. A expansão da conectividade de produtos e serviços pela internet gerou um vasto volume de dados com alto potencial para consumidores, empresas e sociedade em geral.

Dados interoperáveis e de alta qualidade podem ser reutilizados indefinidamente, impulsionando a competitividade, a inovação e o crescimento sustentável. Contudo, desafios como fragmentação de

dados, falta de interoperabilidade e desequilíbrios contratuais dificultam o compartilhamento otimizado de informações.

Principais disposições do Data Act:

- **Acesso do usuário a dados de produtos e serviços conectados:** Regulamenta a disponibilização de dados relativos a um produto ou serviço conectado ao próprio usuário, fortalecendo seus direitos e controle sobre as informações geradas.
- **Disponibilização de dados a terceiros:** Estabelece as condições pelas quais os detentores de dados devem disponibilizá-los a destinatários autorizados, promovendo a concorrência e a inovação.
- **Acesso por organismos públicos:** Prevê a disponibilização de dados a organismos do setor público, à Comissão Europeia, ao Banco Central Europeu e a outros órgãos da UE em situações de necessidade excepcional, para o desempenho de missões de interesse público.
- **Facilitação da portabilidade de serviços de tratamento de dados:** Simplifica a mudança entre diferentes serviços de tratamento de dados, evitando a dependência excessiva de um único fornecedor (lock-in).
- **Proteção contra acesso ilícito:** Introduce salvaguardas contra o acesso não autorizado de terceiros a dados não pessoais, reforçando a segurança e a confiança no ambiente digital.
- **Normas de interoperabilidade:** Promove o desenvolvimento de padrões para garantir que os dados possam ser acessados, transferidos e utilizados de forma eficaz entre diferentes sistemas e plataformas.

Potenciais desafios das regulamentações

Além das oportunidades identificadas, este relatório ressalta os potenciais desafios na implementação das regulamentações Data Governance Act e Data Act, que podem impactar a economia de dados tanto na União Europeia quanto no Brasil. Dentre os principais obstáculos estão questões regulatórias, como a sobreposição de normas que geram falta de clareza jurídica, especialmente na distinção entre dados pessoais e não pessoais conforme o GDPR e o Data Act. Há também conflitos potenciais entre os requisitos de desenvolvimento de produtos exigidos pelo Data Act e os princípios de privacidade e minimização de dados do GDPR. A interação incerta entre o Data Act e outras regulamentações setoriais adiciona complexidade, criando incertezas para empresas em setores altamente regulados.

Desafios comerciais e estruturais também são destacados, incluindo o aumento de custos para fabricantes e fornecedores na adaptação de produtos e serviços, o que pode afetar a competitividade, especialmente das pequenas e médias empresas. A falta de transparência nos preços dos intermediários de dados e as restrições impostas a eles podem desestimular sua atuação no mercado. Além disso, a distribuição desigual de dados e a escassez de profissionais qualificados podem limitar os benefícios da economia de dados. Preocupações com a proteção de propriedade intelectual e a segurança de dados sensíveis reforçam a necessidade de um equilíbrio entre a promoção da inovação e a garantia de privacidade e confiança no ambiente digital.

Benefícios esperados

Além disso, este relatório destaca os benefícios significativos esperados com a implementação das regulamentações Data Governance Act e Data Act. Estudos de impacto preveem um aumento no valor da economia de dados da União Europeia, de **€533,5 bilhões** para um valor estimado entre **€540,7 e €544,4 bilhões** até 2028, representando até **3,95% do PIB** da UE. Ainda, essas regulamentações devem promover a inovação e a eficiência em diversos setores, como saúde, mobilidade, indústria, agricultura, tecnologia e meio ambiente, ao incentivar o compartilhamento seguro de dados e a criação de novos serviços e soluções. Por exemplo, espera-se economias anuais de **€120 bilhões** no setor de saúde e melhorias significativas na eficiência operacional da indústria, potencializando o crescimento econômico e a competitividade.

Por outro lado, a **ausência** de um marco regulatório unificado pode resultar em **perdas substanciais** para a economia de dados. Sem a intervenção coordenada da UE, estimam-se riscos de fragmentação legal e domínio de grandes empresas de tecnologia. A falta de regulamentação pode levar a obstáculos no compartilhamento de dados, altos custos de conformidade para as empresas e atrasos no avanço científico, como evidenciado pelos **€10,2 bilhões** anuais perdidos devido à não conformidade com os padrões FAIR em pesquisas. Portanto, a implementação dessas regulamentações é crucial para evitar a perda de oportunidades econômicas e fortalecer a posição competitiva no mercado global de dados.

1. Introdução

As inovações são fundamentais para assegurar a competitividade de longo prazo das economias e promover a prosperidade social. O crescimento econômico está cada vez mais vinculado ao espaço digital, onde serviços inteligentes e plataformas digitais superam os modelos de negócios tradicionais em lucratividade e escalabilidade. Os dados, peça central dessa inovação digital, impulsionam avanços em setores como manufatura, saúde e sustentabilidade. No entanto, de acordo com a Comissão Europeia, 80% dos dados gerados permanecem subutilizados¹ devido a barreiras como a falta de armazenamento em nuvem, problemas de interoperabilidade e a relutância e insegurança dos proprietários em compartilhá-los.

Diante desse cenário global, diversos países estão implementando marcos regulatórios para fortalecer suas economias de dados, e é importante que o Brasil siga esse caminho. Compreender como essas legislações podem servir de referência é um passo fundamental para a criação de instrumentos legais próprios. A análise do panorama internacional, especialmente as regulamentações da União Europeia (UE), podem oferecer insights valiosos sobre os princípios necessários para desenvolver uma estrutura jurídica eficaz.

Visando promover o crescimento da economia digital da UE e incentivar novos modelos de negócios baseados na confiança e no uso responsável dos dados, a Comissão Europeia introduziu a **Estratégia Europeia de Dados**². O objetivo central dessa iniciativa é criar um mercado único de dados, conhecido como Espaço Comum de Dados, que garanta o uso ético das informações. Para viabilizar essa visão, foram criados vários instrumentos legislativos³, como o **Data Governance Act** e o **Data Act**, que atuam como pilares para atingir os objetivos delineados, e outros regulamentos como o *Digital Services Act*, o *Digital Markets Act* e o *Artificial Intelligence Act* como apresentados na Figura 1.

Este documento apresenta uma análise detalhada do *Data Governance Act* e do *Data Act*, que constituem a base da estrutura regulatória da União Europeia para dados. O estudo explora seus impactos e desafios como um primeiro passo para avaliar a viabilidade de um marco regulatório similar no Brasil. Além disso, inclui uma análise concisa dos princípios subjacentes e dos elementos centrais desses atos, considerando seu impacto potencial em casos de uso comercial de dados em diferentes setores econômicos.

¹ EUROPEAN COMMISSION. Data Act: Commission proposes measures for a fair and innovative data economy. Disponível em: [link](#). Acesso em 27-09-2024.

² EUROPEAN UNION. A European strategy for data. Disponível em: [link](#). Acesso em 02-10-2024.

³ MCKINSEY & COMPANY. The EU digital strategy: The impact of data privacy on global business. Disponível em: [link](#). Acesso 02-10-2024.

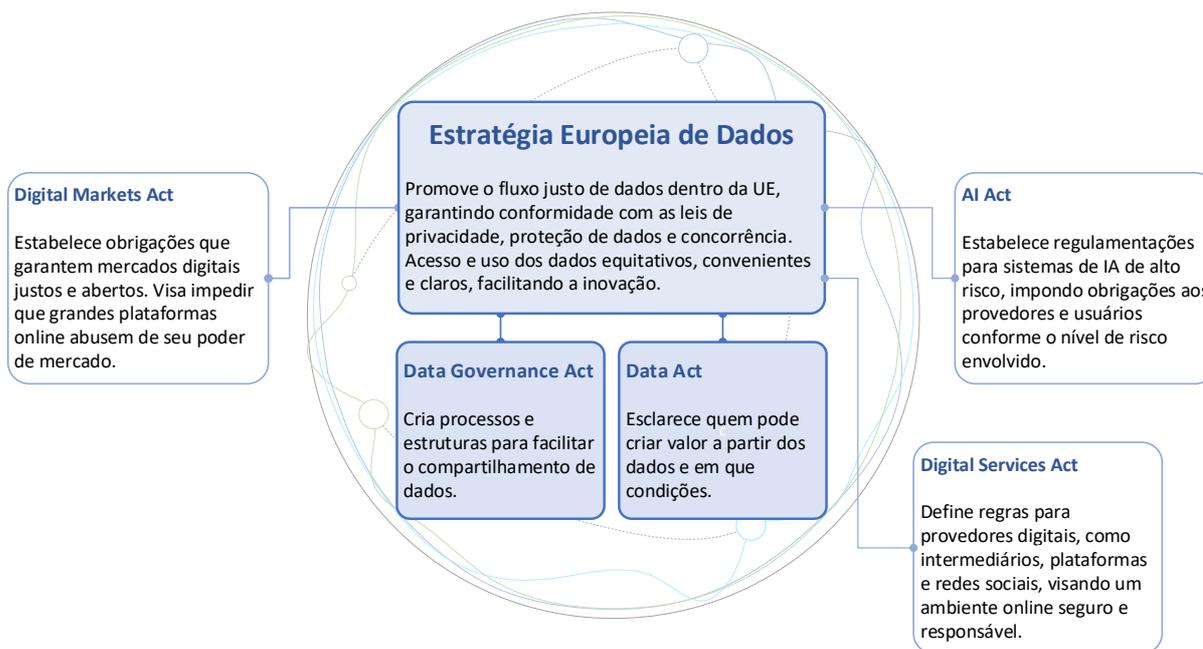
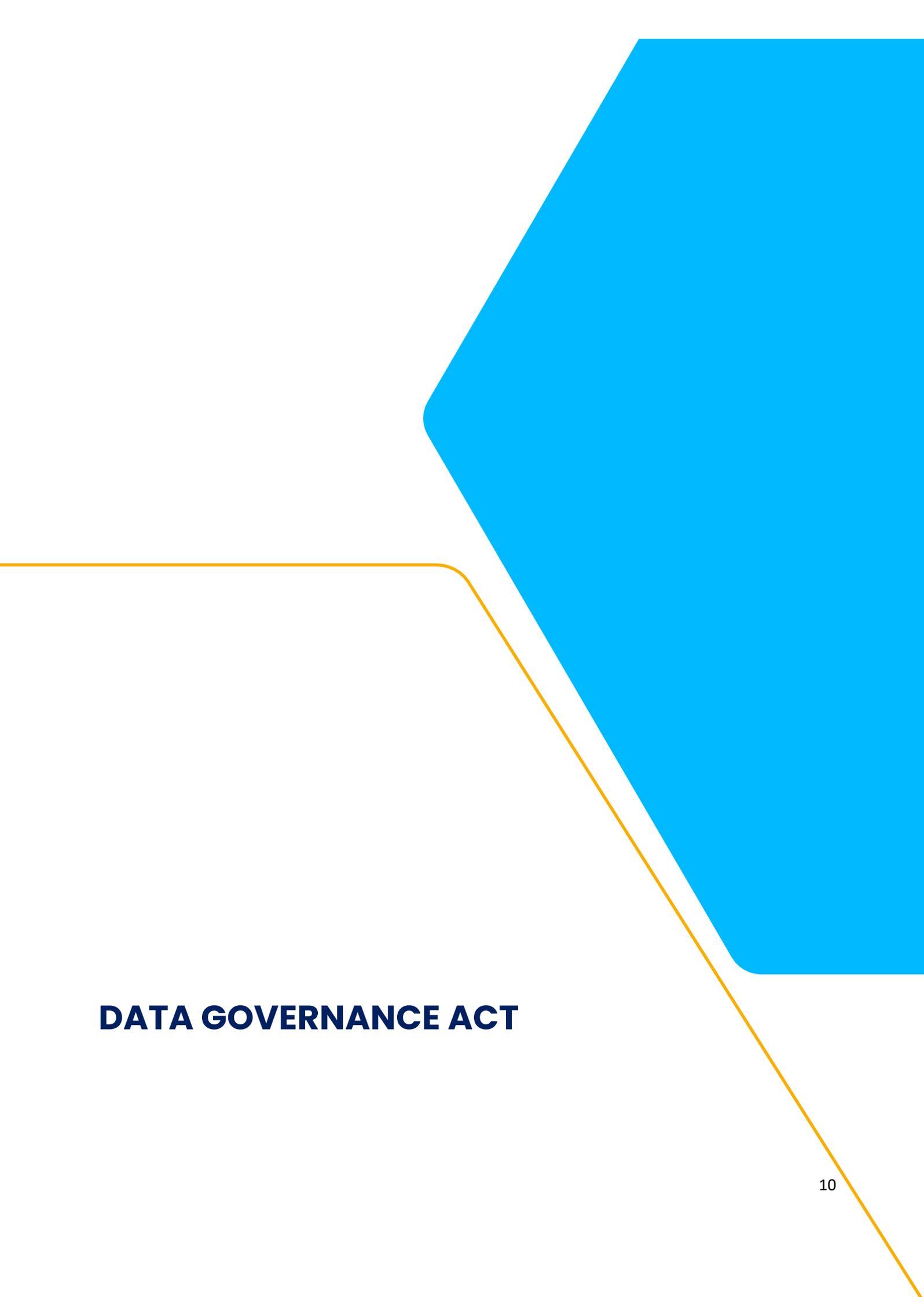


Figura 1 – Estratégia europeia de dados (Fonte: adaptado de RISSANEN et al. (2023))

A large blue polygon is positioned in the upper right quadrant of the page. A thin orange line starts from the left edge of the page, extends horizontally, and then curves downwards and to the right, ending near the bottom right corner.

DATA GOVERNANCE ACT

2. Data Governance Act

O *Data Governance Act* (DGA)⁴ é um dos pilares fundamentais da estratégia europeia para dados, com o objetivo de promover o compartilhamento voluntário e seguro de dados. O DGA estabelece diretrizes de mercado que devem ser seguidas por todos os participantes do mercado europeu, independentemente de sua localização. Dessa forma, a União Europeia busca ampliar o alcance de suas normas além de suas fronteiras, concentrando-se na criação de um mercado único digital e em espaços de dados comuns que impulsionem uma economia digital eficiente e atraente.

Embora o DGA não estabeleça regras específicas para o acesso ou uso de dados, ele foi projetado para enfrentar a concentração de poder das grandes empresas de tecnologia, conhecidas como Big Tech. Seu principal objetivo é garantir que operadores econômicos menores também possam se beneficiar do valor gerado pelos fluxos de dados, criando condições de concorrência mais equitativas. Assim, o DGA atua como um instrumento intersetorial, regulando a reutilização de informações detidas pelo setor público, incentivando o compartilhamento de dados por meio de novos intermediários e promovendo o altruísmo de dados.

De acordo ao **Capítulo I, Artigo 1**, o DGA estabelece:

- As condições para a reutilização de determinadas categorias de dados não abertos, detidos por organismos do setor público (como dados protegidos por regulamentações de propriedade intelectual ou segredos comerciais), não concedem direitos automáticos nem impõem obrigações. Em vez disso, estabelecem uma estrutura que define as condições a serem seguidas caso a reutilização desses dados seja permitida.
- Um regime de notificação e supervisão para a prestação de serviços de intermediação de dados;
- Uma estrutura para o altruísmo de dados, i.e., o compartilhamento de dados voluntariamente e sem recompensa;
- Um regime para a criação de um Comitê Europeu da Inovação de Dados;
- Medidas para permitir o fluxo seguro de dados não pessoais para fora da UE.

2.1. Conceitos

Para facilitar a compreensão dos principais conceitos, o DGA define, no **Capítulo I, Artigo 2**, **dados** como qualquer representação digital de fatos ou informações, incluindo gravações sonoras, visuais ou audiovisuais. Dados pessoais e não pessoais estão incluídos no escopo, onde dados pessoais são aqueles protegidos pelo Regulamento Geral de Proteção de Dados (GDPR)⁵, os demais são dados não pessoais. A **reutilização dos dados** detidos por organismos do setor público se refere à utilização dessas informações por indivíduos ou entidades, para fins comerciais ou não, que não correspondem ao propósito original para o qual os dados foram produzidos. Já, os **serviços de intermediação de dados** são plataformas ou serviços que facilitam as transações de compartilhamento de dados entre detentores e utilizadores de dados, além de auxiliar os titulares dos dados (pessoas ou entidades a quem os dados pertencem) a exercerem seus direitos, especialmente em relação a dados pessoais. O conceito de **altruísmo de dados** envolve a partilha voluntária de dados, baseada no consentimento dos titulares ou na autorização dos detentores, sem a intenção de obter benefícios financeiros além da cobertura de custos. Essa prática visa contribuir para fins de interesse público, como saúde,

⁴ REGULATION (EU) 2022/868.

⁵ REGULATION (EU) 2016/679.

combate às mudanças climáticas, mobilidade, políticas públicas, estatísticas oficiais e pesquisa científica.

2.2. Atores

É importante identificar os **Principais atores** aos quais o regulamento se aplica, sendo estes:

- O **detentor dos dados**, pode ser uma pessoa jurídica, incluindo organismos do setor público e organizações internacionais, ou uma pessoa física que, não sendo o titular dos dados, tem o direito, de acordo com a legislação da União ou a legislação nacional aplicável, de conceder acesso a determinados dados pessoais ou dados não pessoais, ou de compartilhá-los.
- Os **intermediários de dados** são prestadores de serviços que atuam como terceiros neutros, conectando indivíduos e empresas aos usuários de dados. Embora possam cobrar pelo serviço de facilitação do compartilhamento de dados, não têm permissão para utilizar esses dados diretamente com fins lucrativos, como revendê-los a outras empresas ou desenvolver produtos com base neles. Para assegurar essa neutralidade, os intermediários de dados devem cumprir requisitos legais rigorosos, incluindo a separação estrutural entre o serviço de intermediação de dados e quaisquer outras atividades que ofereçam, garantindo que essas operações permaneçam legalmente separadas.
- As **organizações altruístas de dados** são as entidades que facilitam e incentivam o compartilhamento de dados para fins altruístas de forma ética e voluntária.
- O **utilizador dos dados** é qualquer pessoa física ou jurídica que tenha acesso legal a determinados dados pessoais ou não pessoais, e que, conforme estabelecido pelo GDPR (no caso de dados pessoais), tenha o direito de utilizá-los para fins comerciais ou não comerciais.
- Por fim, o órgão criado pelo DGA, o **Comitê Europeu da Inovação de Dados (EDIB)**, tem a função de facilitar o intercâmbio de boas práticas, especialmente no que se refere à intermediação de dados, altruísmo de dados e à utilização de dados públicos que não podem ser disponibilizados como dados abertos. Sendo também responsável por priorizar padrões de interoperabilidade intersetoriais.

2.3. Princípios do Data Governance Act

2.3.1. Confiança

O Regulamento Governança de Dados visa criar instrumentos de confiança que permitam que os dados sejam partilhados de forma fácil em benefício da sociedade.

Conforme o **considerando 19**, tanto empresas quanto titulares dos dados deverão poder ter confiança no fato de que a reutilização de dados protegidos seja feita de forma adequada, preservando seus direitos e interesses.

O regulamento também estabelece um quadro regulamentar para serviços de intermediação de dados (**considerando 32**), garantindo neutralidade e confiança no uso e compartilhamento de dados. Esses intermediários atuam apenas como facilitadores, sem utilizar os dados para outros fins, conforme o **considerando 33**, assegurando o controle total aos detentores de dados.

Para fortalecer a confiança, o **considerando 43** introduz um logotipo comum para identificar prestadores de serviços reconhecidos na União Europeia, permitindo que titulares e detentores saibam com quem estão compartilhando dados. De forma similar, o **considerando 47** introduz um logotipo para organizações de altruísmo de dados, a fim de apoiar os titulares dos dados e os detentores dos dados a identificarem facilmente.

Por fim, embora o DGA possa ajudar a reforçar a autonomia estratégica aberta da União Europeia, também contribui para criar confiança nos fluxos internacionais de dados (**Capítulo VII**).

2.3.2. Consentimento

O princípio de consentimento é fundamental no DGA, assegurando que a partilha de dados ocorra de forma transparente e respeite os direitos dos titulares e detentores de dados. O **considerando 15** destaca que, ao solicitar consentimento ou autorização, os organismos públicos devem informar claramente os titulares ou detentores sobre a possibilidade de recusar a permissão, garantindo uma escolha livre e informada.

O **considerando 45** ressalta que a disponibilização voluntária de dados pelos titulares, com base em consentimento informado, pode servir a objetivos de interesse geral, como saúde pública, mudanças climáticas e mobilidade. Para facilitar esse altruísmo, os Estados-Membros podem estabelecer mecanismos que incentivem a doação de dados, incluindo ferramentas que facilitem a concessão do consentimento.

Conforme o **considerando 50**, o altruísmo de dados deverá se basear no consentimento dos titulares dos dados, conforme definido no GDPR, devendo estar plenamente em conformidade com os requisitos legais dessa regulamentação, assegurando sua legitimidade e transparência.

O **considerando 52** introduz o formulário europeu de consentimento para altruísmo de dados (**Artigo 25**), que visa simplificar a concessão e a retirada do consentimento, especialmente para pesquisa científica e fins estatísticos. Esse formulário oferece clareza e transparência, assegurando que os dados sejam utilizados de acordo com o consentimento dado, enquanto facilita o controle dos titulares sobre a retirada da autorização. A abordagem modular do formulário permite que ele seja adaptado a diferentes setores e objetivos.

2.3.3. Interesse público

O princípio de interesse público no DGA está fortemente relacionado ao altruísmo de dados, conforme descrito no **Capítulo IV**. Esse conceito permite que indivíduos e empresas disponibilizem voluntariamente seus dados, sem remuneração, para fins que promovam o bem comum. A noção de «objetivo de interesse geral» é deixada à definição do direito nacional e existem diferenças entre os Estados-Membros. Exemplos de objetivos de interesse geral incluem cuidados de saúde, combate às mudanças climáticas, melhoria da mobilidade, divulgação de estatísticas oficiais, políticas públicas, prestação de serviços públicos e apoio à pesquisa científica.

2.4. Mecanismos e boas práticas para a partilha de dados

O DGA estabelece mecanismos e boas práticas de compartilhamento de dados, funcionando como um instrumento regulador da reutilização de informações detidas pelo setor público, da mediação de dados por intermediários, da troca voluntária de informações com fins altruístas e das transferências internacionais de dados. A seguir, serão detalhados cada um desses mecanismos, além das funções do Comitê Europeu da Inovação de Dados na promoção de melhores práticas de compartilhamento de dados.

2.4.1. Reutilização de dados detidos pelo Setor Público

A reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público é abordada no **Capítulo II** do DGA. Trata-se de um mecanismo para facilitar a reutilização de certos dados protegidos que não podem ser disponibilizados como dados abertos por motivos de confidencialidade comercial (segredos comerciais, profissionais e empresariais), confidencialidade estatística, proteção dos direitos de propriedade intelectual de terceiros ou proteção de dados pessoais (**Artigo 3**).

Os Estados-Membro devem garantir que os organismos do setor público estejam equipados para proteger a privacidade e a confidencialidade dos dados durante a reutilização. Isso inclui o uso de técnicas como anonimização e ambientes de processamento seguros, além de acordos de confidencialidade. As **condições de reutilização (Artigo 5)** devem ser não discriminatórias, transparentes e justificadas, sem restringir a concorrência. O acesso aos dados deve ser concedido apenas se os dados pessoais forem anonimizados e as informações comerciais confidenciais (por exemplo, segredos comerciais) forem tratadas adequadamente e somente com tal consentimento ou permissão. A reutilização deve ocorrer em ambientes de processamento seguros supervisionados pelo setor público. Os reutilizadores devem manter a confidencialidade, proibir a reidentificação dos titulares dos dados e notificar o organismo público sobre quaisquer violações que possam ocorrer.

Se um órgão do setor público não puder conceder acesso a certos dados para reutilização, deve auxiliar o potencial reutilizador a buscar o consentimento do indivíduo para reutilizar seus dados pessoais ou a permissão do detentor dos dados cujos direitos ou interesses podem ser afetados pela reutilização.

Os órgãos do setor público podem cobrar **taxas (Artigo 6)** pela reutilização de dados, desde que essas taxas não excedam os custos incorridos, além de serem transparentes, não discriminatórias e justificadas. Para fomentar a reutilização em pesquisa científica e em outras atividades não comerciais, bem como por pequenas e médias empresas (PMEs) e startups, os órgãos do setor público devem considerar a redução ou até mesmo a isenção dessas cobranças.

Cada Estado-Membro deve designar um ou mais **organismos competentes (Artigo 7)** para apoiar os órgãos do setor público na concessão ou recusa de acesso à reutilização. Esses organismos poderão fornecer um ambiente de processamento seguro, oferecer orientações sobre como estruturar e armazenar dados de maneira acessível, e prestar apoio técnico para a pseudonimização, entre outras atividades.

Os Estados-Membros devem garantir que todas as informações relevantes estejam disponíveis e acessíveis através de um **ponto de informação único (Artigo 8)**. Esse ponto será responsável por receber pedidos de informação ou solicitações de reutilização. A Comissão Europeia criou o **Registro**

Europeu de Dados Protegidos mantidos pelo setor público (ERPD)⁶, um registro eletrônico pesquisável dos dados disponíveis nos pontos de informação nacionais, além de informações sobre como solicitar dados através desses pontos.

Um órgão do setor público, ou organismo competente deve adotar uma **decisão sobre o pedido de reutilização (Artigo 9)** das categorias de dados no prazo máximo de dois meses a contar da data de solicitação do pedido.

A figura a seguir resume os principais pontos do DGA sobre a reutilização dos dados do setor público.

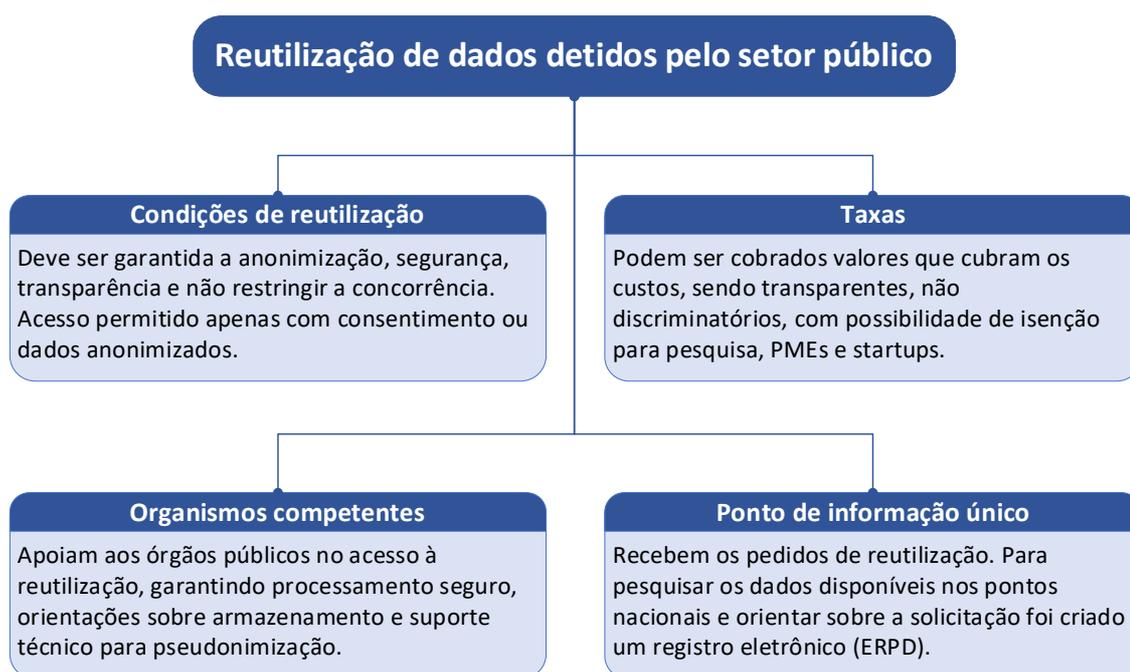


Figura 2 – Reutilização de dados do setor público

2.4.2. Intermediação na partilha de dados

Para aumentar a confiança no compartilhamento de dados, esta nova abordagem propõe um modelo baseado na neutralidade e transparência dos intermediários de dados, ao mesmo tempo em que coloca indivíduos e empresas no controle de seus dados. A estrutura oferece um modelo alternativo às práticas de tratamento de dados das plataformas Big Tech.

O DGA define um conjunto de regras aplicáveis aos **serviços de intermediação de dados (Capítulo III, Artigo 10)** para garantir que os intermediários funcionem como organizadores confiáveis de compartilhamento ou agrupamento de dados dentro dos Espaços Comuns de Dados Europeus. Podem ser serviços de intermediação entre detentores dos dados e potenciais utilizadores de dados, incluindo a disponibilização de meios técnicos ou outros que permitam esses serviços (intercâmbios bilaterais ou multilaterais de dados ou a criação de plataformas ou de bases de dados que permitam o

⁶ EUROPEAN UNION. The European register for protected data held by the public sector (ERPD). Disponível em: [link](#). Acesso em 1-10-2024.

intercâmbio ou a utilização conjunta de dados, bem como a criação de outras infraestruturas específicas para a interligação entre detentores dos dados e utilizadores de dados); serviços de intermediação entre titulares dos dados que procuram disponibilizar os seus dados pessoais, ou pessoas singulares que procuram disponibilizar dados não pessoais, e potenciais utilizadores de dados, incluindo a disponibilização de meios técnicos ou outros que permitam esses serviços e, em particular, que permitam o exercício dos direitos dos titulares dos dados; serviços de cooperativas de dados.

Sob a DGA, os intermediários de dados devem apresentar uma **notificação à autoridade competente (Artigo 11)** sobre sua intenção de fornecer tais serviços. Cada Estado-Membro designa uma ou mais **autoridades competentes (Artigo 13)** para gerir esse processo. A autoridade competente garantirá que o procedimento de notificação seja justo, não discriminatório e que todas as informações necessárias (nome, forma jurídica, endereço, site Web, descrição dos serviços, entre outras), sejam incluídas na notificação. Após o recebimento de tal confirmação, o intermediário de dados pode legalmente começar a operar e usar o rótulo “provedor de serviços de intermediação de dados reconhecido na União”. A fim de garantir que os intermediários reconhecidos na União sejam facilmente identificáveis em toda a União, a Comissão concebe o logotipo comum⁷, e mantém um registro central de intermediários de dados reconhecidos. A autoridade competente pode cobrar taxas pela notificação, proporcionais e baseadas nos custos administrativos associados ao **controle do cumprimento (Artigo 14)** e a outras atividades de controle do mercado realizadas pelas autoridades competentes em matéria de serviços de intermediação de dados.

Para garantir a neutralidade o intermediário de dados está sujeito a uma série de **condições de prestação do serviço** conforme o **Artigo 12**. Primeiramente, não pode usar os dados para outros fins além de disponibilizá-los aos usuários, e deve operar através de uma entidade jurídica distinta. As condições comerciais, como os preços, não devem depender do uso de outros serviços do mesmo prestador ou de entidades relacionadas. O ajuste do formato dos dados só é permitido para melhorar a interoperabilidade ou quando solicitada pelos usuários. O acesso ao serviço deve ser justo, transparente e não discriminatório, garantindo a interoperabilidade com outros serviços por meio de normas abertas. O prestador deve adotar medidas técnicas, legais e organizacionais para prevenir transferências ilegais de dados não pessoais e informar prontamente os detentores de dados sobre acessos não autorizados. Também deve garantir um nível adequado de segurança no armazenamento, processamento e transmissão de dados, especialmente para informações sensíveis. Se o prestador fornece ferramentas para consentimento ou autorização, deve especificar a jurisdição onde os dados serão usados e oferecer instrumentos para dar ou retirar o consentimento. Por fim, deve manter um registro das atividades de intermediação de dados.

Uma **exceção (Artigo 14)** neste mecanismo é que ele não se aplica a organizações de altruísmo de dados ou entidades sem fins lucrativos que colem dados para fins de interesse geral, a menos que elas busquem estabelecer relações comerciais entre titulares e utilizadores de dados.

A figura a seguir ilustra os principais aspectos relacionados à intermediação na partilha de dados.

⁷ EUROPEAN UNION. Logos for data intermediaries and data altruism organisations recognised in the Union. Disponível em: [link](#). Acesso em 1-10-2024.

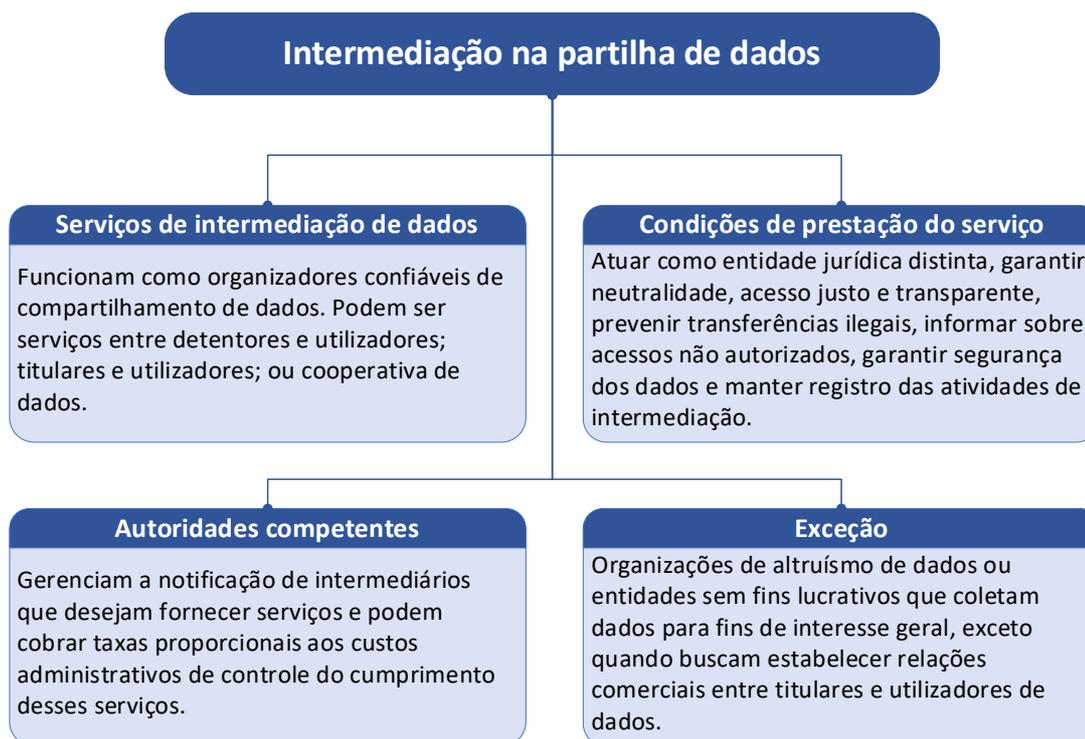


Figura 3 – Intermediação no compartilhamento de dados

2.4.3. Altruísmo de dados

O altruísmo de dados se aplica a indivíduos e empresas que dão seu consentimento ou permissão para disponibilizar dados que eles geram, voluntariamente e sem recompensa, para serem usados para objetivos de interesse geral. Os Estados-Membros podem definir **políticas nacionais para o altruísmo de dados (Artigo 16)** para facilitar aos titulares dos dados a disponibilizarem voluntariamente os dados pessoais e definir as informações necessárias que devem ser prestadas aos titulares dos dados no que diz respeito à reutilização dos seus dados no interesse geral.

De acordo ao **Artigo 18**, para que uma entidade seja registrada como organização de altruísmo de dados reconhecida, ela deve atuar no altruísmo de dados, ser uma pessoa jurídica estabelecida para fins de interesse geral conforme a legislação nacional, operar sem fins lucrativos e ser independente de entidades com fins lucrativos, e realizar suas atividades de altruísmo de dados de forma separada de suas outras funções.

Cada Estado-Membro designa uma ou mais **autoridades competentes (Artigo 23)** responsáveis por manter um **registro público nacional das organizações de altruísmo de dados reconhecidas (Artigo 17)**. Uma vez registrada de acordo ao **Artigo 19**, a entidade pode legalmente começar a operar e usar o título de “organização de altruísmo de dados reconhecida na União”. A Comissão Europeia também cria um logotipo comum⁸ e mantém um registro central para garantir a fácil identificação dessas organizações em toda a União.

⁸ EUROPEAN UNION. Logos for data intermediaries and data altruism organisations recognised in the Union. Disponível em: [link](#). Acesso em 1-10-2024.

As organizações de altruísmo devem cumprir com certos **requisitos de transparência (Artigo 20)**, como manter registros detalhados sobre quem teve acesso aos dados, a duração e finalidade do uso, e as taxas cobradas, se aplicável. Também devem enviar um relatório anual à autoridade competente, que inclua informações sobre suas atividades, como promoveram os fins de interesse geral, uma lista de quem teve acesso aos dados e para quais fins, e detalhes sobre receitas e despesas relacionadas ao acesso aos dados.

As organizações de altruísmo de dados reconhecidas devem atender a **requisitos específicos para salvaguardar os direitos e interesses dos titulares dos dados e dos detentores dos dados no que respeita aos seus dados (Artigo 21)**. Elas devem informar claramente aos titulares ou detentores dos dados sobre os objetivos de interesse geral para os quais os dados serão utilizados. O uso dos dados deve se limitar aos fins autorizados, sem recorrer a práticas enganosas. As organizações de altruísmo de dados devem fornecer ferramentas para facilitar o consentimento e a retirada de autorização, além de garantir a segurança no armazenamento e tratamento dos dados. Em casos de uso não autorizado de dados não pessoais, devem notificar rapidamente os envolvidos.

As autoridades competentes em matéria de registro das organizações de altruísmo de dados **controlam o cumprimento (Artigo 24)**, por parte das organizações de altruísmo de dados reconhecidas, dos requisitos mencionados anteriormente.

O **formulário europeu de consentimento para o altruísmo de dados (Artigo 25)** facilitará a coleta de dados entre Estados-Membros em um formato uniforme. Terá uma abordagem modular para atender setores e finalidades específicas, assegurando que os titulares possam facilmente dar e retirar seu consentimento, conforme os requisitos do GDPR.

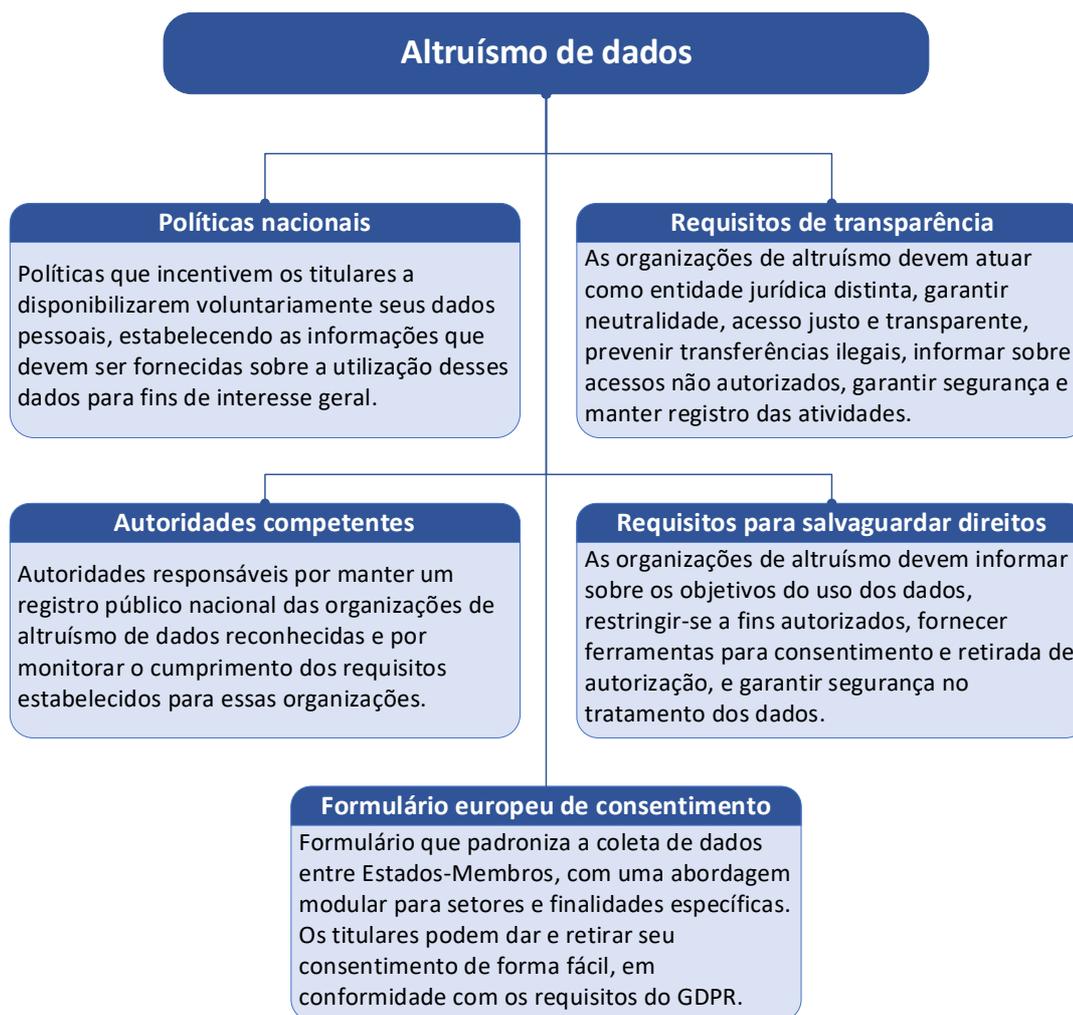


Figura 4 – Altruísmo de dados

2.4.4. Comitê Europeu da Inovação de Dados

O Comitê Europeu da Inovação de Dados (EDIB) foi criado pela Comissão da EU sob a forma de um grupo de peritos, composto por representantes das autoridades competentes dos Estados-Membros para a intermediação de dados e para o altruísmo de dados, do Comitê Europeu para a Proteção de Dados, da Autoridade Europeia para a Proteção de Dados, da Agência da União Europeia para a Cibersegurança (ENISA), da Comissão, o enviado/representante da UE para as PMEs e outros representantes de organismos relevantes selecionados pela Comissão através de um convite à apresentação de peritos (**Artigo 29**).

O EDIB desempenha diversas funções essenciais para o desenvolvimento e a gestão de dados na União Europeia. Entre suas atribuições (**Artigo 30**), se destacam aconselhar e assistir à Comissão na criação de práticas coerentes para a gestão de pedidos de reutilização de dados por organismos do setor público e em matéria de altruísmo de dados e a aplicação de requisitos para prestadores de serviços de intermediação de dados e organizações de altruísmo de dados reconhecidas. O Comitê também é responsável pela elaboração de diretrizes para a proteção de dados não pessoais comercialmente sensíveis e para a segurança cibernética no intercâmbio e armazenamento de dados. Outro aspecto

importante de suas funções é a definição de normas intersetoriais que promovam a interoperabilidade e o intercâmbio de boas práticas entre setores. Para os espaços comuns europeus de dados, o EDIB propõe quadros interoperáveis, garantindo acesso não discriminatório e respeitando as regras de concorrência. Facilita a cooperação entre os Estados-Membros na definição de condições harmonizadas para a reutilização de dados detidos pelo setor público e reforça a colaboração entre as autoridades competentes em matéria de serviços de intermediação de dados. Por fim, o EDIB auxilia na avaliação da necessidade de adoção de atos de execução, na elaboração do formulário europeu de consentimento para altruísmo de dados e na melhoria do quadro regulatório internacional referente a dados não pessoais.

2.4.5. Acesso e transferências internacionais de dados

O **Capítulo VII** do DGA estabelece salvaguardas para proteger dados não pessoais armazenados na UE contra as tentativas de acesso indevido por governos de países terceiros ou transferências internacionais que possam entrar em conflito com a legislação da UE ou de seus Estados-Membros. Para isso, órgãos do setor público, entidades com direito de reutilizar dados, prestadores de serviços de intermediação de dados e organizações de altruísmo de dados devem adotar medidas técnicas, legais e organizacionais para prevenir acessos inadequados ou transferências não autorizadas. Decisões judiciais ou administrativas de governos externos só serão reconhecidas ou executadas caso estejam fundamentadas em um acordo internacional entre a UE (ou seus Estados-Membros) e o país em questão.

Na ausência de tal acordo, uma decisão judicial ou administrativa de um país terceiro que exija acesso aos dados somente poderá ser cumprida se atender a três condições específicas. Primeiro, o pedido deve ser justificado com razões concretas e estar vinculado a um caso específico, como investigações que envolvam suspeitos ou infrações. Em segundo lugar, o destinatário do pedido deve ter o direito de apresentar uma objeção, que será devidamente analisada por um tribunal do país terceiro. Por fim, o tribunal estrangeiro deve reconhecer e respeitar as normas jurídicas europeias ao decidir sobre o acesso aos dados.

Se esses requisitos forem cumpridos, apenas a quantidade mínima de dados permitida deve ser fornecida em resposta ao pedido. Além disso, os titulares dos dados devem ser informados previamente sobre o pedido de acesso aos seus dados, exceto em situações relacionadas à aplicação da lei em que o sigilo seja indispensável para a eficácia das investigações.

NOTA: O **Artigo 27** garante que as pessoas e entidades tem o ***direito de reclamação*** à autoridade competente sobre prestadores de serviços de intermediação de dados ou organizações de altruísmo de dados. A autoridade responsável deve informar o autor da reclamação sobre o andamento e a decisão tomada. Por sua vez, se uma autoridade competente não atender a uma reclamação, qualquer pessoa ou entidade afetada tem o ***direito à ação judicial (Artigo 28)*** ou solicitar uma reavaliação por um organismo imparcial com a devida competência técnica.

A large blue polygon is positioned in the upper right quadrant of the page. A thin orange line starts horizontally from the left edge of the page, then curves downwards and to the right, ending near the bottom right corner.

DATA ACT

3. Data Act

O *Data Act*⁹ é uma regulamentação que complementa o *Data Governance Act* dentro da estratégia europeia de dados. Enquanto o *Data Governance Act* aumenta a confiança em mecanismos de compartilhamento de dados, o *Data Act* fornece clareza jurídica em relação ao acesso e uso de dados pessoais e não pessoais, contribuindo para a criação de um mercado único de dados na UE. A crescente conectividade de produtos e serviços através da Internet gerou um vasto volume de dados com grande potencial para consumidores, empresas e a sociedade. Esses dados, quando interoperáveis e de alta qualidade, podem ser reutilizados ilimitadamente, impulsionando a competitividade, inovação e crescimento sustentável. No entanto, diversos obstáculos, como a fragmentação de dados, falta de interoperabilidade e desequilíbrios contratuais, impedem a otimização no compartilhamento de dados. Para superar essas barreiras, o *Data Act* estabelece um regime harmonizado que define quem pode acessar e utilizar dados gerados por **produtos e serviços conectados**, assim como as condições e fundamentos que regem esse acesso.

No **Capítulo I, Artigo 1**, o regulamento define as principais regras que regem o acesso e a disponibilização de dados, abrangendo os seguintes aspectos:

- A disponibilização de dados relativos a um produto ou serviço conexo ao usuário do produto conectado ou do serviço conexo;
- A disponibilização de dados pelos detentores dos dados aos destinatários dos dados;
- A disponibilização de dados pelos detentores dos dados a organismos do setor público, à Comissão, ao Banco Central Europeu e aos órgãos da União, quando haja uma necessidade excepcional desses dados, para o desempenho de uma missão específica de interesse público.

Assim, considerando os três aspectos mencionados, a transferência de dados, conforme o *Data Act*, é ilustrada na Figura 5.

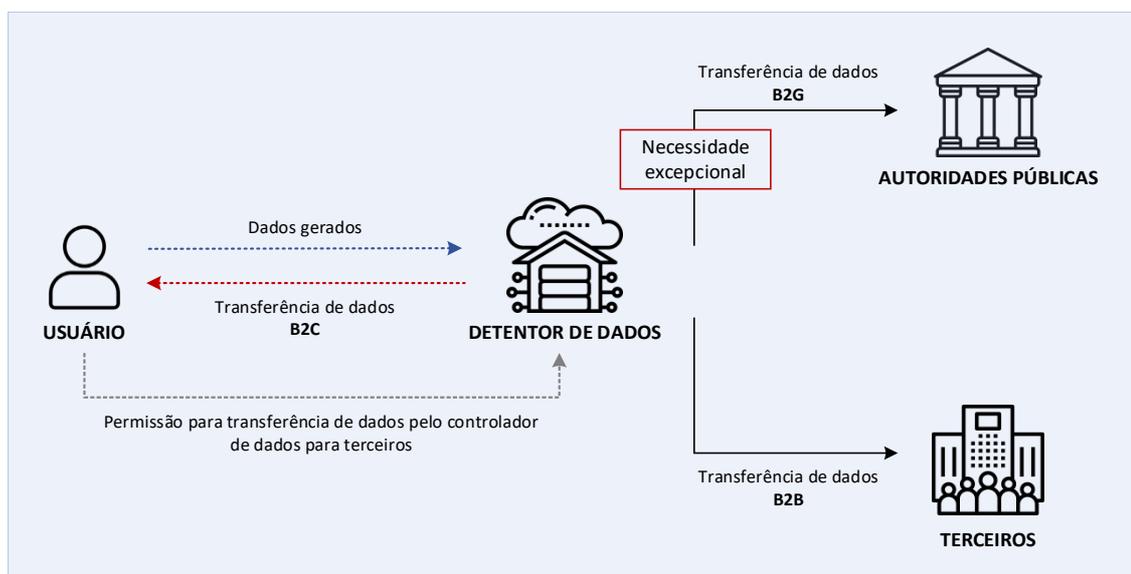


Figura 5 – Transferência de dados de acordo com o Data Act (Fonte: adaptado de DELOITTE (2024))

⁹ REGULATION (EU) 2023/2854.

A continuação, são apresentados dois exemplos¹⁰ breves para um melhor entendimento da transferência de dados de acordo ao *Data Act*.

Exemplo 1: o usuário do produto conectado é o titular dos dados, e o terceiro é uma empresa privada:

O motorista de um carro conectado é tanto usuário quanto o titular dos dados gerados durante o uso do veículo. A empresa fabricante do carro atua como a detentora desses dados, coletando informações sobre padrões de direção com base em um contrato com o usuário. O motorista autoriza o fabricante a compartilhar essas informações com sua seguradora. Com acesso a esses dados, a seguradora pode analisar o comportamento de direção e oferecer descontos nos prêmios de seguro para motoristas que demonstram práticas de direção seguras, incentivando uma condução mais responsável e proporcionando economia aos usuários.

Exemplo 2: O usuário de um produto conectado não é o titular dos dados, e uma autoridade pública enfrenta uma necessidade excepcional:

Um paciente é monitorado por seu médico usando um termômetro conectado. O paciente é o titular dos dados, e o médico é o usuário do dispositivo. Com o aumento de casos de uma doença na comunidade, uma autoridade de saúde decide coletar dados para entender a disseminação do vírus. A empresa de tecnologia, como detentora dos dados, compartilhará as informações de temperatura do paciente com a autoridade de saúde, com o consentimento do médico e dos pacientes, em um contexto de emergência para responder à crise de saúde.

Finalmente, o regulamento também aborda os seguintes pontos:

- A **facilitação da mudança** entre serviços de tratamento de dados;
- A introdução de **salvaguardas contra o acesso ilícito** de terceiros a dados não pessoais;
- O desenvolvimento de **normas de interoperabilidade** para os dados a que se pretenda aceder e que se pretenda transferir e utilizar.

3.1. Conceitos

Para facilitar a compreensão, é essencial definir os conceitos de produtos conectados e serviços relacionados. Conforme o **Capítulo I, Artigo 2:**

- um **produto conectado** é um bem que obtém, gera ou recolhe dados relativos à sua utilização ou ao seu ambiente e que é capaz de comunicar dados relativos a um produto através de um serviço de comunicações eletrônicas, de uma conexão física ou do acesso no dispositivo, e cuja função principal não consiste na conservação, no tratamento ou na transmissão de dados em nome de quaisquer partes que não sejam o utilizador.
- um **serviço relacionado** é um serviço digital conectado ao produto no momento da aquisição ou locação de tal modo que a sua ausência impediria que o produto conectado desempenhasse uma ou mais das suas funções, ou conectado posteriormente ao produto

¹⁰ DELOITTE. The EU Data Act: What does it mean for you? – Deloitte Luxembourg – Technology. Disponível em: [link](#). Acesso em 27-09-2024.

pelo fabricante ou por terceiros, a fim de aumentar, atualizar ou adaptar as funções do produto conectado.

3.2. Atores

É igualmente fundamental identificar quem serão os responsáveis pelo uso e acesso a esses dados. Dessa forma, os **Principais atores** envolvidos no regulamento incluem:

- os **usuários**, que podem ser pessoas físicas ou jurídicas que possui, aluga ou arrenda um produto conectado ou recebe um serviço relacionado.
- Outro ator são os **detentores de dados**, que geralmente é a empresa que fabrica o produto conectado ou que fornece um serviço relacionado, e que tem a capacidade de disponibilizar de determinados dados através de um contrato com o usuário.
- Por fim, os **terceiros** que são aqueles que recebem os dados do detentor dos dados a pedido do usuário, para finalidades relacionadas ao seu negócio comercial ou profissão, mas sem ser o próprio usuário do produto ou serviço.

Além dos atores principais, o regulamento é aplicável a outros atores, como os **organismos do setor público**, que solicitam aos detentores dos dados que os disponibilizem quando exista uma necessidade excepcional. Os **prestadores de serviços de tratamento de dados**, independentemente do seu local de estabelecimento, que prestam esses serviços a clientes na União. Os **participantes em espaços de dados** e as pessoas cuja atividade implique a implantação de contratos inteligentes para terceiros no contexto da execução de um acordo.

3.3. Princípios do Data Act

3.3.1. Soberania de dados

O princípio da soberania de dados garante aos usuários o direito de controlar e acessar os dados gerados por dispositivos conectados e serviços associados. Esse princípio é abordado no **Artigo 3**, que estabelece a obrigação de que os dados sejam facilmente acessíveis aos usuários. O artigo determina que produtos e serviços devem ser projetados para garantir que os dados e metadados sejam disponibilizados de forma simples, segura e gratuita, preferencialmente em um formato estruturado e legível automaticamente. Isso assegura que os cidadãos possam utilizar seus dados para diversos fins, incluindo o desenvolvimento de novos serviços e melhorias em produtos

3.3.2. Acesso equitativo a dados

O princípio de acesso equitativo a dados busca equilibrar o acesso a dados entre grandes corporações e PMEs. O considerando 40 reconhece que empresas em fase de startup, pequenas e médias empresas, assim como empresas de setores tradicionais com capacidades digitais limitadas, enfrentam dificuldades para acessar dados relevantes. O regulamento visa facilitar esse acesso para essas entidades, garantindo que as obrigações impostas a elas sejam proporcionais, evitando assim a sobrecarga regulatória.

3.3.3. *Transparência e confiança*

O princípio de transparência e confiança é essencial para garantir a equidade e a responsabilidade nas relações entre detentores de dados e usuários. Conforme o considerando 51, a transparência **assegura que a compensação** exigida por detentores de dados seja razoável. O Artigo 28 estabelece obrigações de transparência contratual, enquanto o Artigo 27 enfatiza o dever de **boa-fé**, exigindo que todas as partes cooperem para facilitar a transferência de dados e manter a continuidade dos serviços de tratamento.

Além disso, o considerando 96 menciona **cláusulas contratuais-tipo benéficas**, para aumentar a confiança nos serviços de tratamento de dados, promovendo uma relação mais equilibrada entre usuários e prestadores. O considerando 102 destaca a importância de **salvaguardas que assegurem o controle dos dados** pelos cidadãos e entidades da União, respeitando direitos e normas sobre segurança, proteção de dados e privacidade. Para prevenir acessos governamentais ilegais a dados não pessoais, os prestadores de serviços de tratamento devem adotar medidas adequadas, como criptografia e auditorias frequentes, garantindo assim a proteção e a confiança dos usuários em relação ao tratamento de seus dados.

3.3.4. *Interoperabilidade*

O princípio de interoperabilidade enfatiza a importância de permitir que dados e serviços interajam de maneira eficiente entre diferentes participantes dentro dos espaços de dados. O **Capítulo VIII** do regulamento aborda especificamente a interoperabilidade, direcionando-se a todos os envolvidos na oferta de dados ou serviços baseados em dados, incluindo fornecedores de contratos inteligentes e provedores de serviços de processamento de dados. Os prestadores de serviços de tratamento de dados devem atender a requisitos que **facilitem a interoperabilidade**, permitindo a utilização simultânea de diferentes serviços de tratamento de dados (**Artigo 34**). As especificações de interoperabilidade aberta e normas harmonizadas devem abordar aspectos como a interoperabilidade do transporte, sintática, semântica, comportamental e das políticas (**Artigo 35**).

Os aspectos técnicos da interoperabilidade são tratados no **Capítulo VI** e incluem a necessidade de os prestadores de serviços de tratamento de dados **assegurarem a compatibilidade** com especificações comuns, baseando-se em normas de interoperabilidade abertas ou harmonizadas (**Artigo 30**).

3.3.5. *Portabilidade de dados*

O princípio de portabilidade de dados, fundamentado nas diretrizes do GDPR, é um aspecto central do *Data Act*. Ele permite que os **titulares de dados transfiram suas informações** entre diferentes controladores que oferecem serviços concorrentes, aumentando a flexibilidade e o controle dos consumidores sobre seus dados. Embora o GDPR restrinja o direito à portabilidade a dados pessoais processados em certas bases legais e com viabilidade técnica, o *Data Act* amplia esse direito para incluir dados gerados por produtos conectados. Isso significa que os consumidores poderão acessar e transferir não apenas dados pessoais, mas também não pessoais, gerados por esses produtos (**Artigo 1**).

O considerando 20 menciona que, apesar das intenções positivas, muitos dados gerados por produtos conectados não são facilmente acessíveis, limitando efetivamente a portabilidade. O *Data Act* aborda

essa questão, buscando melhorar a situação e garantir que os direitos dos titulares de dados sejam respeitados, mesmo diante de exceções.

De acordo com o considerando 31, as exceções aos direitos de acesso não devem afetar o direito à portabilidade dos dados, conforme estipulado pelo GDPR.

O considerando 79 enfatiza a necessidade de **códigos de conduta que promovam a portabilidade** de dados e a mudança de prestadores de serviços. Dada a baixa adesão a esses códigos, o regulamento propõe a implementação de **obrigações mínimas** para eliminar obstáculos que dificultam a transferência de dados, como questões técnicas, contratuais e organizativas.

O **Artigo 30** estipula que prestadores de serviços de tratamento de dados devem oferecer interfaces abertas a todos os clientes, **facilitando a mudança de serviços e a portabilidade** de dados. Essas interfaces devem fornecer informações suficientes para o desenvolvimento de software que suporte à interoperabilidade.

Outro ponto importante é a **criação de especificações e normas de interoperabilidade** abertas, que são essenciais para um ambiente de computação em nuvem entre vários provedores. De acordo ao **Artigo 35**, essas especificações devem abordar aspectos como a portabilidade sintática e semântica dos dados, além da compatibilidade entre aplicações e políticas associadas.

3.4. Papel dos atores para o acesso e uso de dados

Para garantir que se compreenda como cada ator envolvido no contexto do *Data Act* pode e deve atuar, a seguir são abordados os direitos e obrigações de cada um. Com o cumprimento das obrigações e o exercício dos direitos, busca-se assegurar o acesso e uso de dados que garantam os princípios anteriormente mencionados.

3.4.1. Usuários

Os usuários dos produtos conectados ou serviços relacionados tem **direito** a:

- **Acesso aos dados de produtos e serviços conectados (Artigo 3)**: Os usuários devem ter acesso fácil, seguro e gratuito aos dados de produtos e serviços conectados, em formatos comuns e estruturados.
- **Limitação de uso de dados (Artigo 4)**: Os usuários têm o direito de limitar ou proibir, por meio de contratos, o acesso, uso ou compartilhamento posterior de seus dados, especialmente se isso comprometer a segurança do produto conectado.
- **Compartilhamento de dados com terceiros (Artigo 5)**: Usuários podem compartilhar diretamente dados com terceiros ou podem solicitar que os dados sejam compartilhados com terceiros, e o detentor deve disponibilizá-los de forma rápida e segura.

3.4.2. Detentores de dados

Os detentores de dados, segundo o regulamento, dispõem dos seguintes **direitos**:

- **Uso de dados não pessoais (Artigo 4)**: Os detentores de dados podem usar apenas dados não pessoais que estejam prontamente disponíveis, baseando-se em contratos com os usuários.

- **Confidencialidade de segredos comerciais (Artigo 4):** Os segredos comerciais devem ser mantidos em sigilo e só podem ser revelados se medidas de proteção forem acordadas entre o detentor e o usuário. Caso não haja acordo ou o usuário comprometa a confidencialidade, o detentor pode reter ou suspender a partilha desses dados.
- **Limitação de uso de dados (Artigo 4):** Os detentores também podem limitar ou proibir, contratualmente, o acesso, uso ou compartilhamento de dados que possam comprometer a segurança do produto conectado.
- **Compensação pela disponibilização de dados (Artigo 9):** Os detentores de dados que tem uma obrigação legal sob a lei da UE ou nacional de disponibilizar dados para terceiros, podem solicitar uma compensação do destinatário dos dados, que deve ser não discriminatória e razoável, podendo incluir uma margem.
- **Medidas técnicas de proteção (Artigo 11):** Os detentores podem implementar medidas técnicas para proteger os dados, como contratos inteligentes e criptografia. No entanto, essas medidas não podem discriminar entre os destinatários ou prejudicar o direito do usuário de acessar seus dados.

Os detentores são responsáveis por atender às seguintes **obrigações**:

- **Acessibilidade dos dados (Artigo 4):** Os detentores devem garantir que os dados e metadados estejam acessíveis ao usuário sem atrasos injustificados, com qualidade equivalente àquela que eles têm, de forma fácil, segura e gratuita, em um formato comum.
- **Disponibilização de dados a terceiros (Artigo 5):** Quando solicitado, os detentores devem compartilhar dados e metadados com terceiros de forma segura e sem atrasos.
- **Garantia de uso para finalidades acordadas (Artigo 6):** Os detentores devem assegurar que os terceiros utilizem os dados apenas para os fins previamente acordados.
- **Condições de compartilhamento (Artigo 8):** O detentor deve estabelecer termos justos, razoáveis e não discriminatórios para a disponibilização de dados a terceiros, de maneira transparente, conforme as diretrizes do regulamento.
- **Demandas de uso excepcional por organismos públicos (Artigo 14):** Caso órgãos do setor público ou entidades da UE demonstrem necessidade excepcional de determinados dados, os detentores não públicos devem disponibilizá-los mediante solicitação devidamente justificada.

3.4.3. Terceiros

Conforme estabelecido no regulamento, os terceiros têm o seguinte **direito**:

- **Recebimento de dados (Artigo 5):** Terceiros têm o direito de receber dados do detentor a pedido do usuário, incluindo metadados, de forma rápida, segura e gratuita.

Os terceiros têm a seguinte **obrigação** a cumprir:

- **Uso acordado e proteção de dados pessoais (Artigo 6):** Devem utilizar os dados apenas para as finalidades acordadas e respeitar as normas de proteção de dados da UE, eliminando dados desnecessários, a menos que haja acordo contrário para dados não pessoais.

3.4.4. Organismos do setor público

Os organismos do setor público, a Comissão Europeia, o Banco Central Europeu ou outra entidade da União têm **direito** a:

- **Acesso em necessidade excepcional (Artigo 14)**: Têm direito a dados em situações de necessidade excepcional, mediante pedido fundamentado. Essa necessidade excepcional pode incluir, por exemplo, emergências públicas ou de interesse público quando os dados não puderem ser obtidos por outros meios (**Artigo 15**).

E devem atender à seguinte **obrigação**:

- **Uso exclusivo e segurança (Artigo 19)**: Devem usar os dados apenas para as finalidades solicitadas, aplicando medidas de segurança para garantir a confidencialidade e os dados devem ser excluídos quando não forem mais necessários.

3.4.5. Prestadores de serviços de tratamento de dados

Os prestadores de serviços são responsáveis por atender às seguintes **obrigações**:

- **Facilitação de migração (Artigo 23)**: Devem permitir a migração para outros serviços ou infraestrutura local, eliminando obstáculos pré-comerciais, comerciais, técnicos, contratuais e organizativos.
- **Informação ao cliente (Artigo 26)**: Devem fornecer informações claras sobre procedimentos de migração e transferência de dados.
- **Compatibilidade técnica (Artigo 30)**: Devem garantir a compatibilidade com normas abertas para facilitar a interoperabilidade.
- **Interoperabilidade (Artigo 35)**: Prestadores de serviços de dados devem garantir a interoperabilidade e portabilidade em nuvem, tanto para dados quanto para aplicações, abrangendo aspectos sintáticos, semânticos, comportamentais e de políticas.

3.4.6. Participantes de espaços de dados

Os participantes em espaços de dados que oferecem dados ou serviços de dados a outros participantes devem cumprir os seguintes requisitos:

- **Partilha de dados e interoperabilidade (Artigo 33)**: Participantes devem descrever dados, restrições e formatos de forma acessível e automatizada. Devem também garantir o acesso técnico via APIs, permitindo compartilhamento contínuo ou em tempo real, além de assegurar a interoperabilidade de ferramentas automatizadas, como contratos inteligentes.

3.4.7. Implementadores de contratos inteligentes

As pessoas ou empresas cuja atividade implique a implantação de contratos inteligentes para terceiros no contexto da execução de um acordo devem garantir:

- **Requisitos para contratos inteligentes (Artigo 36)**: Devem ser sólidos, com controle de acesso rigoroso e resistência a falhas e manipulações. Devem incluir mecanismos seguros de cessação e interrupção, com auditabilidade e arquivamento dos dados. Precisam estar

alinhados com os termos do acordo de compartilhamento de dados, assegurando sua coerência e continuidade das operações.

3.4.8. Órgãos de implementação

Para garantir a execução eficaz do regulamento, cada Estado-Membro deve designar uma ou mais **autoridades competentes** (**Capítulo IX, Artigo 37**). Essas autoridades têm diversas **funções**, incluindo a promoção da literacia de dados, o tratamento de reclamações sobre infrações ao regulamento (como a violação de segredos comerciais), a realização de investigações, a imposição de sanções financeiras e a monitorização da evolução tecnológica e comercial relevante para o uso de dados. Além disso, elas cooperam com outras autoridades nacionais e internacionais para garantir a aplicação consistente do regulamento em toda a UE. Podem ser novas ou já existentes, caso houver várias autoridades competentes, os Estados-Membros devem designar uma delas como **coordenador de dados**. O coordenador de dados **atuará como um "balcão único"** para todas as questões relacionadas à implementação do *Data Act* em nível nacional, facilitando sua aplicação tanto para empresas quanto para autoridades públicas. As autoridades competentes devem atuar de forma imparcial, livres de influências externas, e não podem receber instruções de entidades públicas ou privadas em casos individuais.

Para a coordenação da aplicação do *Data Act* foi criado um grupo de especialistas da Comissão, o **Comitê Europeu da Inovação de Dados** (**Artigo 42**). Este comitê apoia a Comissão, fornecendo orientações e assistências às autoridades competentes, facilitando a cooperação entre elas e ajudando no desenvolvimento de normas e diretrizes harmonizadas para assegurar a interoperabilidade e práticas comuns para o funcionamento dos espaços de dados. Ele também atua na coordenação de sanções e na gestão de casos transfronteiriços, promovendo uma aplicação coerente do regulamento em toda a União Europeia.

NOTA: O **Artigo 38** garante que indivíduos ou empresas tem **direito de reclamação** às autoridades competentes de seu país de residência, trabalho ou estabelecimento, caso considerem seus direitos violados. O coordenador de dados deve fornecer informações necessárias para isso. Por sua vez, o **Artigo 39** assegura que qualquer pessoa afetada pode recorrer à justiça contra decisões das autoridades competentes. Se uma reclamação não for atendida, há o **direito à ação judicial** ou revisão por um órgão imparcial.

A large blue polygon is positioned in the upper right quadrant of the page. A yellow line starts from the left edge, extends horizontally, then curves downwards and to the right, ending near the bottom right corner.

POTENCIAIS DESAFIOS

4. Potenciais desafios das regulamentações

Nesta seção são apresentadas opiniões de especialistas e entidades sobre os desafios da implementação das regulamentações *Data Governance Act* e *Data Act*. Caso não resolvidos, estes poderiam significar impactos negativos na economia da UE ou na implementação efetiva das regulamentações.

4.1. Desafios regulatórios

Os principais desafios regulatórios¹¹ emergem da sobreposição de regulamentações da UE que não oferecem a clareza necessária. A seguir, são apresentados alguns desses desafios identificados.

Um desafio de privacidade identificado é a **separação de dados pessoais e não pessoais**, conforme o GDPR e o *Data Act*. O GDPR tem uma definição ampla de dados pessoais, que podem incluir informações que identifiquem indiretamente um indivíduo, como uma placa de carro. Por outro lado, produtos conectados e serviços relacionados, geram dados mistos, exigindo que dados pessoais sejam separados e tratados sob diferentes regimes jurídicos.

Existe outro potencial conflito de **desenvolvimento de produtos** entre o *Data Act*, que exige que os dados sejam facilmente acessíveis aos usuários, e o GDPR, que promove a privacidade desde a concepção e a minimização da coleta de dados para finalidades específicas.

A dificuldade na aplicação dos **direitos dos titulares dos dados**, devido a que sob o *Data Act*, o usuário nem sempre é o titular dos dados, o que torna desafiador determinar quando aplicar os direitos dos titulares de dados do GDPR, em contraste com os direitos de acesso previstos pelo *Data Act*.

Outro desafio de privacidade envolve **dados de categorias especiais**, como os de saúde, gerados por tecnologias de "internet das pessoas", como os *Smart Watches*. Esses dados são considerados mais sensíveis e têm proteção adicional sob o GDPR, mas não são abordados explicitamente no *Data Act*. Isso gera um risco de conflito entre os dois regimes e dificulta a conformidade ao lidar com dados que podem implicar obrigações em ambas as legislações.

As **transferências internacionais de dados** também poderiam significar um desafio, já que o *Data Act* exige que provedores de nuvem impeçam o acesso estrangeiro a dados não pessoais armazenados na UE, exceto quando tal acesso for permitido por acordos internacionais. Embora o *Data Act*, estabeleça essas restrições para proteger os dados contra acessos não autorizados, há incerteza sobre sua aplicação, uma vez que os dados não pessoais não estão sujeitos às regras de transferências internacionais da UE e do Reino Unido.

A **interação entre o Data Act e outras regulamentações setoriais** é incerta. Por exemplo, tecnologias médicas já estão sujeitas a legislações existentes, como os Regulamentos de Dispositivos Médicos. A falta de clareza sobre como os requisitos do *Data Act* se alinharão a essas normas gera incertezas para empresas que operam em setores altamente regulados.

Um desafio potencial entre o GDPR e o DGA é que este último permite que o titular dos dados conceda acesso ou compartilhe seus dados com um número ilimitado de terceiros para fins não especializados, o que contraria o **princípio de limitação de finalidade** do GDPR. Essa discrepância pode comprometer a proteção dos dados pessoais.

¹¹ FIELDFISHER DATA & PRIVACY TEAM. Privacy Series: The EU Data Act. Disponível em: [link](#). Acesso em 20-09-2024.

4.2. Desafios comerciais

Os novos regulamentos trazem desafios comerciais¹² que impactam nos custos e competitividade no mercado. A seguir, são apresentados alguns desses possíveis desafios.

Os fabricantes e fornecedores de produtos e serviços abrangidos pelo *Data Act* podem enfrentar um **aumento nos custos** de pesquisa e desenvolvimento (P&D), desenvolvimento de produtos e conformidade. Para garantir o direito de acesso aos dados dos usuários, será necessário ajustar o design dos produtos, permitindo a extração e a disponibilização de todos os dados gerados durante o uso, o que pode exigir investimentos substanciais.

Um desafio do DGA é garantir a **não discriminação e a transparência nos preços** cobrados pelos intermediários de dados. A falta de clareza nas tarifas pode prejudicar a competitividade e a confiança entre as partes envolvidas, criando um ambiente desfavorável para o compartilhamento de dados.

Os intermediários de dados enfrentarão um regime de notificação ao fornecer serviços de compartilhamento, além de **obrigações fiduciárias**. O DGA não oferece benefícios claros para intermediários, impondo diversos deveres legais que podem desestimular a sua atuação neste mercado. Ainda, o DGA impede que intermediários de dados utilizem estes dados para benefício próprio ou em negócios não exclusivamente relacionados à intermediação.

A **complexidade do tratamento de dados** é um desafio significativo no DGA, com a imposição de numerosos deveres adicionais que as empresas devem cumprir para oferecer serviços de compartilhamento. Essa carga pode ser mais facilmente gerenciada por grandes empresas, tornando-se um obstáculo para as PMEs que desejam participar desse mercado.

4.3. Desafios estruturais

A implementação da economia de dados enfrenta obstáculos¹³ que podem comprometer seu pleno desenvolvimento, como os desafios identificados a seguir.

A potencial **distribuição desigual de dados** pode exacerbar desigualdades já existentes, caso determinados grupos ou regiões sejam excluídos dos benefícios gerados.

Outro desafio é a **escassez de pessoal qualificado**, que pode dificultar a implementação de projetos baseados em dados. A economia de dados exige profissionais especializados com expertise em áreas como análise de dados, inteligência artificial e aprendizado de máquina, competências fundamentais para o sucesso desses projetos.

¹² FIELDFISHER DATA & PRIVACY TEAM. Privacy Series: The EU Data Act. Disponível em: [link](#). Acesso em 20-09-2024.

¹³ VDMA. Quick Guide: Interoperability Interface Standards for Applying the EU Data Act Successfully. Disponível em: [link](#). Acesso em 02-10-2024.

4.4. Desafios de privacidade

Em meio de um cenário regulatório complexo, surgem alguns desafios de privacidade¹⁴, apresentados a continuação.

Um desafio no *Data Act* é a incerteza sobre o **tratamento de dados sensíveis** das empresas após a divulgação. Mesmo com medidas contratuais, há preocupações sobre o controle de dados compartilhados com terceiros.

As novas obrigações de compartilhamento de dados podem comprometer a **proteção de ativos de propriedade intelectual** (PI) essenciais. Sob o *Data Act*, as empresas enfrentam o risco de exposição de segredos comerciais, levantando preocupações sobre como salvaguardar informações críticas e manter a competitividade em um mercado cada vez mais colaborativo.

¹⁴ FIELDFISHER DATA & PRIVACY TEAM. Privacy Series: The EU Data Act. Disponível em: [link](#). Acesso em 20-09-2024.

A large, solid blue polygon is positioned in the upper right quadrant of the page. A thin yellow line starts from the left edge of the page, extends horizontally, then curves downwards and to the right, ending near the bottom right corner.

POTENCIAIS BENEFÍCIOS

5. Benefícios esperados

O estudo de Avaliação de Impacto da proposta do *Data Governance Act*¹⁵ considera como linha de base o valor econômico total da economia de dados para a UE-27 em 2020, estimado em €325 bilhões (2,6% do PIB). Nesse estudo foram avaliadas duas opções de políticas, uma opção regulatória de baixa intensidade e outra de alta intensidade. Segundo as previsões, para 2028, o valor da economia de dados sem intervenção seria de €533,5 bilhões (3,87% do PIB). Com uma intervenção regulatória, com base em análises de custo-benefício e multicritério (eficácia, eficiência, coerência, viabilidade jurídica/política e proporcionalidade), o estudo prevê que, até 2028, o valor da economia de dados da UE alcance entre 540,7 e 544,4 bilhões de euros (3,92% a 3,95% do PIB).

Um estudo semelhante foi realizado para a Avaliação de Impacto da proposta do *Data Act*¹⁶, no qual foram considerados três opções de políticas:

- A opção 1 propunha intervenção mínima com medidas não vinculativas para melhorar o acesso e o uso de dados;
- A opção 2 sugeria um conjunto limitado de medidas legislativas para facilitar o uso de dados e garantir maior segurança jurídica sobre como e por quem podem ser usados;
- A opção 3 incluía obrigações mais amplas para o uso de dados por empresas terceirizadas, consumidores e órgãos do setor público, bem como disposições mais fortes nas obrigações dos provedores de serviços e os requisitos de interoperabilidade.

De acordo as análises a opção 2 foi escolhida como a preferida, pois aumentaria a certeza jurídica sobre os dados, ampliaria sua reutilização e daria maior controle a consumidores e empresas, mantendo baixos os custos de acesso aos dados. Além disso, promoveria a padronização da interoperabilidade técnica e aumentaria o PIB da UE-27 em 1,98% até 2028, além de impulsionar receitas governamentais e investimentos em €96,8 bilhões e €30,4 bilhões, respectivamente, entre 2024 e 2028.

Além do impacto econômico direto na economia de dados, as regulamentações do *Data Governance Act (DGA)* e do *Data Act* procuram trazer benefícios em diferentes setores. Esses impactos derivam do incentivo ao compartilhamento de dados entre empresas e setores, o que impulsiona a inovação, abrindo espaço para novos serviços e soluções que antes não eram possíveis. As regulamentações também promovem um uso mais eficiente dos dados, permitindo otimizar operações, identificar oportunidades de melhoria e reduzir desperdícios, seja em tempo, recursos ou custos. Ao mesmo tempo, garantem que esses dados sejam utilizados de forma ética e segura, prevenindo abusos e estabelecendo um ambiente de confiança entre todos os envolvidos.

¹⁵ EUROPEAN UNION. IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (*Data Governance Act*). Disponível em: [link](#). Acesso em 07-10-2024.

¹⁶ EUROPEAN UNION. IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (*Data Act*). Disponível em: [link](#). Acesso em 07-10-2024.

A tabela a seguir apresenta uma visão geral desses impactos, organizados por setor e divididos em consequências qualitativas e quantitativas.

Tabela 1 – Impactos do Data Act e do DGA

Setor	Regulação	Impactos	
		Qualitativos	Quantitativos
 Saúde	DGA	Melhor tratamento personalizado e maior qualidade de cuidados	Economia de €120 bilhões por ano no setor de saúde da UE ¹⁷
	Data Act	Alocação eficiente de recursos, serviços de reparação e manutenção de dispositivos médicos	Combate à malária pode economizar até €5 bilhões em custos de saúde globalmente ¹⁸
 Mobilidade	DGA	Redução de tempo em transportes públicos a partir do uso de dados de mobilidade	Economia de mais de 27 milhões de horas de usuários de transporte público e até €20 bilhões anuais em custos trabalhistas ¹⁷
	Data Act	Notificação de atrasos de trens em tempo real a partir do uso de dados de mobilidade	Economia de até 27 milhões de horas e €740 milhões em custos trabalhistas ¹⁸
 Administração Pública	DGA	Decisões baseadas em evidências, gerando estatísticas oficiais mais confiáveis ¹⁷	Aumento do valor econômico dos dados em até €11 bilhões até 2028 ¹⁹
	Data Act	Facilitar a utilização de dados detidos para fins de interesse público	Redução dos encargos administrativos em até 155 milhões de euros por ano ²⁰

¹⁷ EUROPEAN UNION. Data governance act. Disponível em: [link](#). Acesso em 30-09-2024.

¹⁸ EUROPEAN UNION. European data strategy. Disponível em: [link](#). Acesso em 27-09-2024.

¹⁹ EUROPEAN INSTITUTE OF PUBLIC ADMINISTRATION. The Data Governance Act: Breaking down the strategy for data. Disponível em: [link](#). Acesso em 27-09-2024.

²⁰EUROPEAN UNION. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: [link](#). Acesso em 08-10-2024.

Tabela 2 (continuação) – Impactos do Data Act e do DGA

 Indústria	Data Act	<p>Melhor eficiência operacional e redução de recursos graças à acessibilidade a dados de desempenho de equipamentos industriais²¹</p> <p>Reequilibrar a distribuição do valor dos dados entre os atores do mercado, reforçando a capacidade de competir das PMEs²²</p>	<p>Disponibilidade de dados para uso comercial e inovação entre empresas geraria até €196,7 bilhões por ano até 2028²²</p> <p>Crescimento de 33 para 175 zettabytes até 2025, gerando €270 bilhões adicionais no PIB na UE27 até 2028²³</p> <p>Crescimento da produtividade entre 5% e 10% mais rápido para as empresas que investem em inovação baseada em dados²⁴</p> <p>Aumento dos lucros das PMEs em aproximadamente €5,2 bilhões por ano, devido à correção do desequilíbrio nas relações contratuais bilaterais²²</p>
 Agricultura	DGA	Desenvolvimento da agricultura de precisão, novos produtos no setor agroalimentar e novos serviços nas áreas rurais ²⁵	
	Data Act	Aumentar a produtividade e otimizar as condições de cultivo, como clima, temperatura, umidade, preços de mercado e localização GPS, a partir da análise em tempo real de dados dos equipamentos conectados (IoT) dos produtores ²¹	
 Tecnologia	Data Act	Redução de custos para mover dados para outros provedores de nuvem e salvaguarda contra-transferências ilegais de dados ²⁶	O valor e os serviços da Internet das coisas até 2030 representarão €5 a €10 a nível mundial ²⁴
 Clima e Meio Ambiente	DGA	Combate às mudanças climáticas, contribuição na redução de emissões de CO ₂ e gestão de emergências (enchentes, incêndios florestais) a partir de dados ambientais ²⁵	

²¹ EUROPEAN UNION. Data Act — Shaping Europe’s digital future. Disponível em: [link](#). Acesso 1-10-2024.

²² EUROPEAN UNION. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: [link](#). Acesso em 08-10-2024.

²³ EUROPEAN COMMISSION. Data Act: measures for a fair and innovative data economy. Disponível em: [link](#). Acesso em 27-09-2024.

²⁴ EUROPEAN UNION. Data Act — Factsheet — Shaping Europe’s digital future. Disponível em: [link](#). Acesso em 26-09-2024.

²⁵ EUROPEAN UNION. Data governance act. Disponível em: [link](#). Acesso em 30-09-2024.

²⁶ EUROPEAN UNION. European data strategy. Disponível em: [link](#). Acesso em 27-09-2024.

6. Perdas por falta de regulamentações

Sem a intervenção da UE para a criação de regulamentações sobre uso dos dados, a economia de dados continuaria a crescer para uma estimativa de 533,5 bilhões de euros em 2028. No entanto, com a crescente digitalização da economia e da sociedade, existe o risco de os Estados-Membros legislarem de forma descoordenada sobre questões relacionadas aos dados, o que intensificaria a fragmentação do mercado interno. Por exemplo, os Estados-Membros poderiam adotar legislações nacionais ou setoriais sobre a reutilização de dados de empresas por organismos do setor público, o que, embora aumentasse o volume de dados reutilizados, também aumentaria a fragmentação jurídica e os custos para as empresas²⁷. Além disso, os problemas de interoperabilidade entre setores e Estados-Membros provavelmente persistiriam, enquanto os detentores de dados não teriam incentivo para assegurar a qualidade e precisão de seus dados.

Sem um modelo europeu alternativo, haveria o risco de hegemonia das Big Techs, que já coletam grandes volumes de dados. Essas empresas poderiam consolidar ainda mais sua posição, controlando o acesso aos dados e expandindo suas atividades para setores como saúde, seguros e finanças. Isso poderia limitar os ganhos de produtividade, especialmente em setores tradicionais que estão passando por transformações impulsionadas pela inovação orientada por dados.

Iniciativas nacionais e impulsionadas pela indústria surgiriam em setores essenciais, como manufatura na Alemanha e França, ou agricultura na Holanda. No entanto, essas iniciativas teriam impacto limitado, já que as empresas tenderiam a ser cautelosas quanto ao compartilhamento de dados, enfrentando altos custos para fazê-lo por conta própria ou dependendo de fornecedores de tecnologia com maior poder de negociação, ou startups com menor visibilidade.

Indivíduos poderiam ser incentivados a disponibilizar seus dados de forma altruísta, por exemplo, em iniciativas de pesquisa. No entanto, sem meios confiáveis para facilitar esse processo, as dificuldades relacionadas à reutilização de conjuntos de dados contendo informações pessoais continuariam sem solução. Pesquisadores enfrentariam incertezas ao obter consentimento para esses fins, o que poderia gerar hesitação e, conseqüentemente, atrasos no progresso científico. A falta de conformidade dos dados de pesquisa com os padrões estabelecidos pela iniciativa FAIR (que visa tornar os dados de pesquisa localizáveis, acessíveis, interoperáveis e reutilizáveis) é estimada em um custo de 10,2 bilhões de euros por ano na Europa²⁸.

De acordo com a OCDE²⁹, indivíduos, empresas e governos frequentemente enfrentam barreiras no acesso e uso de dados mantidos por outros, muitas vezes agravadas pela relutância em compartilhá-los. Portanto, a criação de estruturas e mecanismos de governança que promovam uma abordagem coordenada ao uso de dados em todos os setores e Estados-Membros seria fundamental para permitir que as partes interessadas na economia de dados capitalizassem o

²⁷ EUROPEAN UNION. IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: [link](#). Acesso em 07-10-2024.

²⁸ PWC EU SERVICES. Cost of not having FAIR research data (2018).

²⁹ OECD (2019).

potencial do mercado interno. Sem regulamentação sobre o acesso a dados, não haveria garantias de condições equitativas entre provedores nem de liberdade de escolha para os consumidores.

Na consulta pública sobre a estratégia europeia para dados de 2020³⁰, 86,4% dos entrevistados concordaram que mecanismos de governança são necessários para capturar o potencial dos dados, especialmente no uso intersetorial, o que destaca a importância da intervenção da UE para estabelecer uma abordagem coordenada ao compartilhamento de dados.

Esse cenário mostra o grande potencial inexplorado³¹ para reforçar a liderança da Europa por meio da partilha de dados. Para enfrentar esse desafio, a UE precisa ajudar as suas indústrias a desenvolver infraestrutura e conhecimentos em ciência de dados, além de criar quadros regulatórios que permitam e incentivem a partilha de dados, garantindo ao mesmo tempo a segurança e a privacidade.

³⁰ EUROPEAN UNION. Summary report of the public consultation on the European strategy for data. Disponível em: [link](#). Acesso em 07-10-2024.

³¹ EUROPEAN COMMISSION. Shaping the digital transformation in Europe. Disponível em: [link](#). Acesso em 07-10-2024.

7. Conclusões

Este relatório analisou as regulamentações da União Europeia com o objetivo de identificar os principais aspectos, princípios, atores e regras que podem servir de referência para a criação de uma economia de dados no Brasil. Foram examinados os elementos centrais do *Data Governance Act*, que estabelece mecanismos para o compartilhamento de dados, incluindo a reutilização de dados públicos, a intermediação de dados para fins comerciais, o compartilhamento voluntário com propósitos altruístas e as transferências internacionais, além de promover boas práticas na troca de dados.

Também foram discutidos os principais pontos do *Data Act*, que define regras para o acesso e uso de dados por diversos atores, como usuários de produtos conectados, detentores de dados, terceiros autorizados, organismos públicos e participantes de espaços de dados, entre outros.

O estudo identificou, ainda, desafios regulatórios, comerciais, estruturais e de privacidade, bem como os impactos qualitativos e quantitativos esperados dessas regulamentações na economia de dados da UE. Esses impactos podem, de forma proporcional, surgir em países que adotem ou planejem regulamentações semelhantes.

Em resumo, este relatório oferece uma visão clara e abrangente dessas duas regulamentações, fornecendo uma base sólida para a compreensão dos principais fatores a serem considerados no desenvolvimento de um marco regulatório eficiente para dados no Brasil.

8. Referências

DELOITTE. The EU Data Act: What does it mean for you? – Deloitte Luxembourg – Technology. Disponível em: [<https://www.deloitte.com/lu/en/Industries/technology/perspectives/the-eu-data-act-what-does-it-mean-for-you.html>]. Acesso em: 27 set. 2024.

EUROPEAN COMMISSION. Data Act: Commission proposes measures for a fair and innovative data economy. Disponível em: [https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113]. Acesso em: 27 set. 2024.

EUROPEAN COMMISSION. Directorate-General for Communications Networks, Content and Technology, Shaping the digital transformation in Europe. Disponível em: [<https://data.europa.eu/doi/10.2759/294260>]. Publications Office, 2020.

EUROPEAN INSTITUTE OF PUBLIC ADMINISTRATION. The Data Governance Act: Breaking down the strategy for data. Disponível em: [<https://www.eipa.eu/blog/the-data-governance-act-breaking-down-the-strategy-for-data/>]. Acesso em: 27 set. 2024.

EUROPEAN UNION. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A European strategy for data. Disponível em: [<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0066>]. Acesso em: 2 out. 2024.

EUROPEAN UNION. Data Act — Shaping Europe’s digital future. Disponível em: [<https://digital-strategy.ec.europa.eu/en/policies/data-act>]. Acesso em: 1 out. 2024.

EUROPEAN UNION. Data Act — Factsheet — Shaping Europe’s digital future. Disponível em: [<https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet>]. Acesso em: 29 set. 2024.

EUROPEAN UNION. Data Act explained – Shaping Europe’s digital future. Disponível em: [<https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>]. Acesso em: 23 set. 2024.

EUROPEAN UNION. Data governance act – Shaping Europe’s digital future. Disponível em: [<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>]. Acesso em: 30 set. 2024.

EUROPEAN UNION. Data Governance Act explained – Shaping Europe’s digital future. Disponível em: [<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>]. Acesso em: 25 set. 2024.

EUROPEAN UNION. European data strategy. europa.eu, 8 dez. 2022. Disponível em: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en]. Acesso em: 27 set. 2024

EUROPEAN UNION. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: [<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022SC0035>]. Acesso em: 8 out. 2024.

EUROPEAN UNION. IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act). Disponível em: [<https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52020SC0295>]. Acesso em: 7 out. 2024.

EUROPEAN UNION. IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: [<https://ec.europa.eu/newsroom/dae/redirection/document/83524>]. Acesso em: 7 out. 2024.

EUROPEAN UNION. Logos for data intermediaries and data altruism organisations recognised in the Union. Disponível em: [<https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union>]. Acesso em: 1 out. 2024.

EUROPEAN UNION. The European register for protected data held by the public sector (ERPD). Disponível em: [<https://data.europa.eu/data/datasets?superCatalogue=erpd&locale=em>]. Acesso em: 1 out. 2024.

EUROPEAN UNION. Summary report of the public consultation on the European strategy for data. Disponível em: [<https://digital-strategy.ec.europa.eu/en/library/summary-report-public-consultation-european-strategy-data>]. Acesso em: 7 out. 2024.

FIELD FISHER DATA & PRIVACY TEAM. Privacy Series: The EU Data Act. Disponível em: [<https://www.youtube.com/watch?v=SkRmqrmqdf0&list=PLHnh6gEVEJKlwf61s-Mf4qRjB3-cTLsm9&index=8>]. Acesso em: 30 set. 2024.

MCKINSEY & COMPANY. The EU digital strategy: The impact of data privacy on global business – McKinsey. Disponível em: [<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-eu-digital-strategy-the-impact-of-data-privacy-on-global-business>]. Acesso em: 2 out. 2024.

OECD. Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies. [s.l.] OECD Publishing, 2019.

PWC EU SERVICES. Cost of not having FAIR research data. Publications Office of the European Union, 2018.

REGULATION (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724. Data Governance Act. Disponível em: [<http://data.europa.eu/eli/reg/2022/868/oj>]. Acesso em: 20 set. 2024.

REGULATION (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828. Data Act. Disponível em: [<http://data.europa.eu/eli/reg/2022/868/oj>]. Acesso em: 20 set. 2024.

RISSANEN, R. et al. Handbook of cross-border data exchange within the Nordic and Baltic countries. [s.l.] Nordic Council of Ministers, 2023.

VDMA. Quick Guide: Interoperability Interface Standards for Applying the EU Data Act Successfully. Disponível em: [https://www.vdma.org/documents/34570/80333104/Quick+Guide_EN_Interoperability+Inter

face+Standards+for+Applying+the+EU+Data+Act+Successfully.pdf/578ccf60-1a6f-f0c5-2273-e3de7d852153?t=1724066640323]. Acesso em: 2 out. 2024.



Departamento de Engenharia de Produção e Transportes

Universidade Federal do Rio Grande do Sul

Av. Osvaldo Aranha, 99 - 5º andar

90035-190 – Porto Alegre, RS – Brasil

Fone: +55 51 3308.3490

E-mail: neo@producao.ufrgs.br

www.ufrgs.br/neo

