

2021 SUMMER SCHOOL

Towards a Digital Transformation & Innovation in Latin America

30 November 2021

# SESSION 7: TRUST, PRIVACY AND SAFETY ONLINE

---

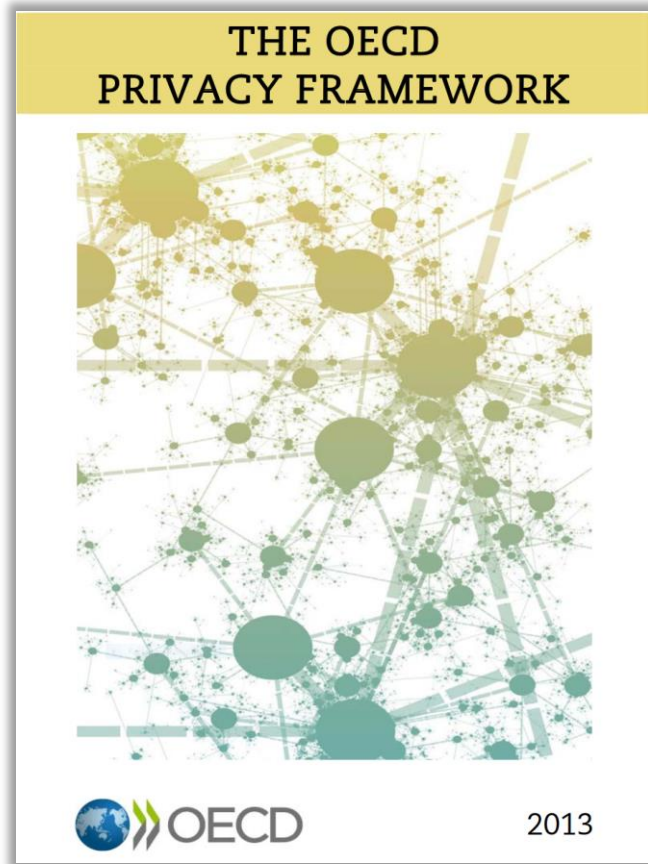
Focusing on the OECD Council Recommendation  
on Enhancing Access to and Sharing of Data

[Christian.Reimsbach-Kounatze@oecd.org](mailto:Christian.Reimsbach-Kounatze@oecd.org)

Twitter: @chreko

# The OECD Working Party on Data Governance and Privacy (WPDGP)

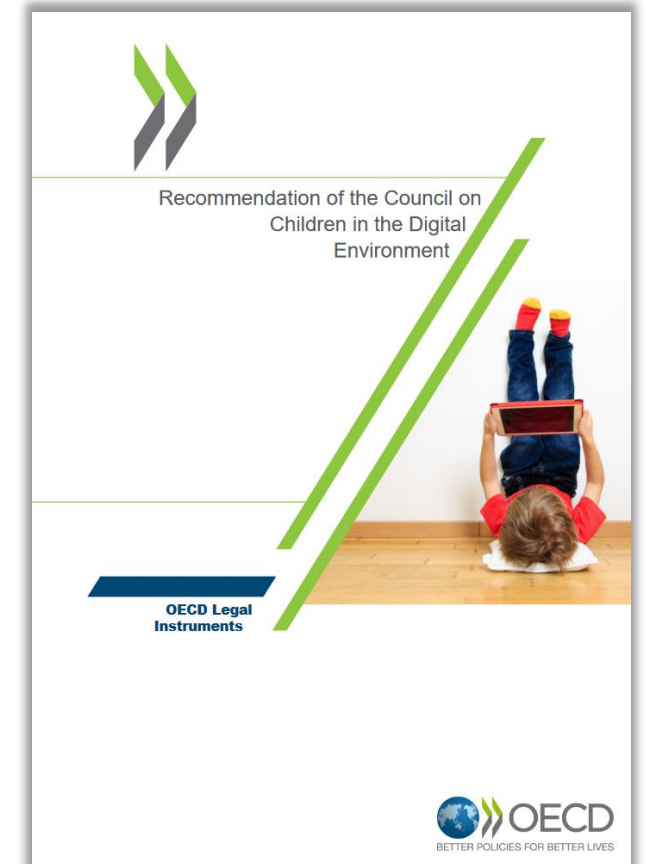
Three major areas of work covered by WPDGP



Privacy



Data access & sharing



Children online

# WPDGP work on data governance and privacy in the context of COVID-19



## Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics

### Key messages

- Digital technologies, in particular mobile and biometric, are being used in innovative ways to improve the effectiveness of public health measures. The resulting information and trends are invaluable for outbreak, warn vulnerable communities, and understand distancing and confinement.
- Disclosures of personal information can allow the public health authorities to track the spread over time. However, containment have varying implications for privacy and data protection.
- Fully transparent and accountable privacy-preserving mechanisms to balance the benefits and the risks associated with data sharing. Data should be retained only for so long as for which it was collected.

### Governments are collaborating with telecoms to access geolocation data to track population

As COVID-19 continues to take human lives and jolt the world, governments are seeking innovative new tools to inform policy and tackle the data are emerging to help authorities monitor and contain the virus. Call data records (CDRs), i.e. data produced by telecommunications companies, are being used to track population movements.

TRACKING AND TRACING COVID: PROTECTING PRIVACY AND DATA



## Rastreo y seguimiento del COVID-19: protección de la privacidad y los datos en el uso de aplicaciones y biometría

Actualizado el 23 de abril de 2020

Las aplicaciones móviles y biométricas, se están adoptando a gran escala para mejorar la eficacia de las respuestas gubernamentales de primera línea.

Estas aplicaciones son invaluable para los gobiernos que buscan rastrear y controlar la propagación del COVID-19, advertir a las comunidades vulnerables y comprender el impacto de las políticas como el distanciamiento social y el confinamiento. Sin embargo, la divulgación de información personal puede permitir que el público identifique más fácilmente posibles infecciones por COVID-19 y acompañe a la propagación a lo largo del tiempo. No obstante, las soluciones digitales para el rastreo y el seguimiento deben incorporar mecanismos de protección de datos.

Las autoridades responsables de preservar la privacidad deben ser transparentes y contar con el consentimiento de los ciudadanos para el intercambio de datos personales y el intercambio de datos personales sea necesario para cumplir con los objetivos de salud pública.

- Así como las tecnologías digitales, en particular aplicaciones móviles y biométricas, están siendo utilizadas de forma innovadora para mejorar la eficacia de las respuestas gubernamentales en la línea de frente de combate al COVID-19.
- Las autoridades responsables de preservar la privacidad deben ser transparentes y contar con el consentimiento de los ciudadanos para el intercambio de datos personales y el intercambio de datos personales sea necesario para cumplir con los objetivos de salud pública.
- Las autoridades responsables de preservar la privacidad deben ser transparentes y contar con el consentimiento de los ciudadanos para el intercambio de datos personales y el intercambio de datos personales sea necesario para cumplir con los objetivos de salud pública.

publicaciones de la OCDE



Version 14 April 2020

## Ensuring data privacy as we battle COVID-19

### Key messages

- Many governments are taking unprecedented measures of the novel coronavirus (COVID-19) by turning to digital technologies to collect, process and share data for effective front-line responses to the virus. While the exceptional measures implemented or proposed to limit the spread of the virus, in terms of their risk of violating privacy and other rights, are necessary, transparency and public consultation are essential to ensure that authorities have generally established a clear legal basis for data protection and privacy during the crisis (recognition that measures are proportional to the risk and a commitment to transparency is over).

TITLE COVID-19 © OECD 2020

Updated 11 August 2020



## Garantizar la privacidad de datos mientras luchamos contra el COVID-19

14 abril 2020

Las autoridades responsables de preservar la privacidad de los ciudadanos han contextualizado en tiempos de crisis o de emergencia, y han aplicado la ley, recordando que el respeto a los principios de protección de datos no obstaculiza la implementación de medidas excepcionales implementadas o previstas por algunos países para limitar la propagación del virus, algunas medidas de riesgos que presentan para la privacidad y otros derechos sobre todo cuando esas medidas carecen de transparencia.

Las autoridades responsables de preservar la privacidad de los ciudadanos han contextualizado en tiempos de crisis o de emergencia, y han aplicado la ley, recordando que el respeto a los principios de protección de datos no obstaculiza la implementación de medidas excepcionales implementadas o previstas por algunos países para limitar la propagación del virus, algunas medidas de riesgos que presentan para la privacidad y otros derechos sobre todo cuando esas medidas carecen de transparencia.

LUCHAMOS CONTRA EL COVID-19 © OECD 2020

publicaciones de la OCDE



## Rastreamento e monitoramento da COVID: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria

### Mensagens principais

- As tecnologias digitais, em particular aplicações móveis e biométricas, estão sendo utilizadas de forma inovadora para melhorar a eficácia das respostas governamentais na linha de frente de combate à COVID-19.
- As informações e tendências resultantes são inestimáveis para os governos que procuram monitorar o surto da COVID-19, alertar comunidades vulneráveis e compreender o impacto de políticas como distanciamento social e confinamento.
- A divulgação de informações pessoais pode permitir que o público identifique mais facilmente possíveis infecções por COVID-19 e acompanhe a propagação ao longo do tempo. No entanto, as soluções digitais para rastreamento e contenção devem incorporar mecanismos de proteção de dados.
- Soluções responsáveis e transparentes de preservação da privacidade devem ser implementadas para garantir que as autoridades responsáveis por preservar a privacidade tenham a confiança dos cidadãos para o compartilhamento de dados pessoais e o compartilhamento de dados pessoais seja necessário para cumprir com os objetivos de saúde pública.

As autoridades responsáveis de preservar a privacidade de los cidadãos han contextualizado en tiempos de crisis o de emergencia, y han aplicado la ley, recordando que el respeto a los principios de protección de datos no obstaculiza la implementación de medidas excepcionales implementadas o previstas por algunos países para limitar la propagación del virus, algunas medidas de riesgos que presentan para la privacidad y otros derechos sobre todo cuando esas medidas carecen de transparencia.

As autoridades responsables de preservar la privacidad de los ciudadanos han contextualizado en tiempos de crisis o de emergencia, y han aplicado la ley, recordando que el respeto a los principios de protección de datos no obstaculiza la implementación de medidas excepcionales implementadas o previstas por algunos países para limitar la propagación del virus, algunas medidas de riesgos que presentan para la privacidad y otros derechos sobre todo cuando esas medidas carecen de transparencia.

publicaciones de la OCDE



## Combating COVID-19's effect on children

publicaciones de la OCDE



## Garantir a privacidade de dados na luta contra a COVID-19

### Mensagens principais

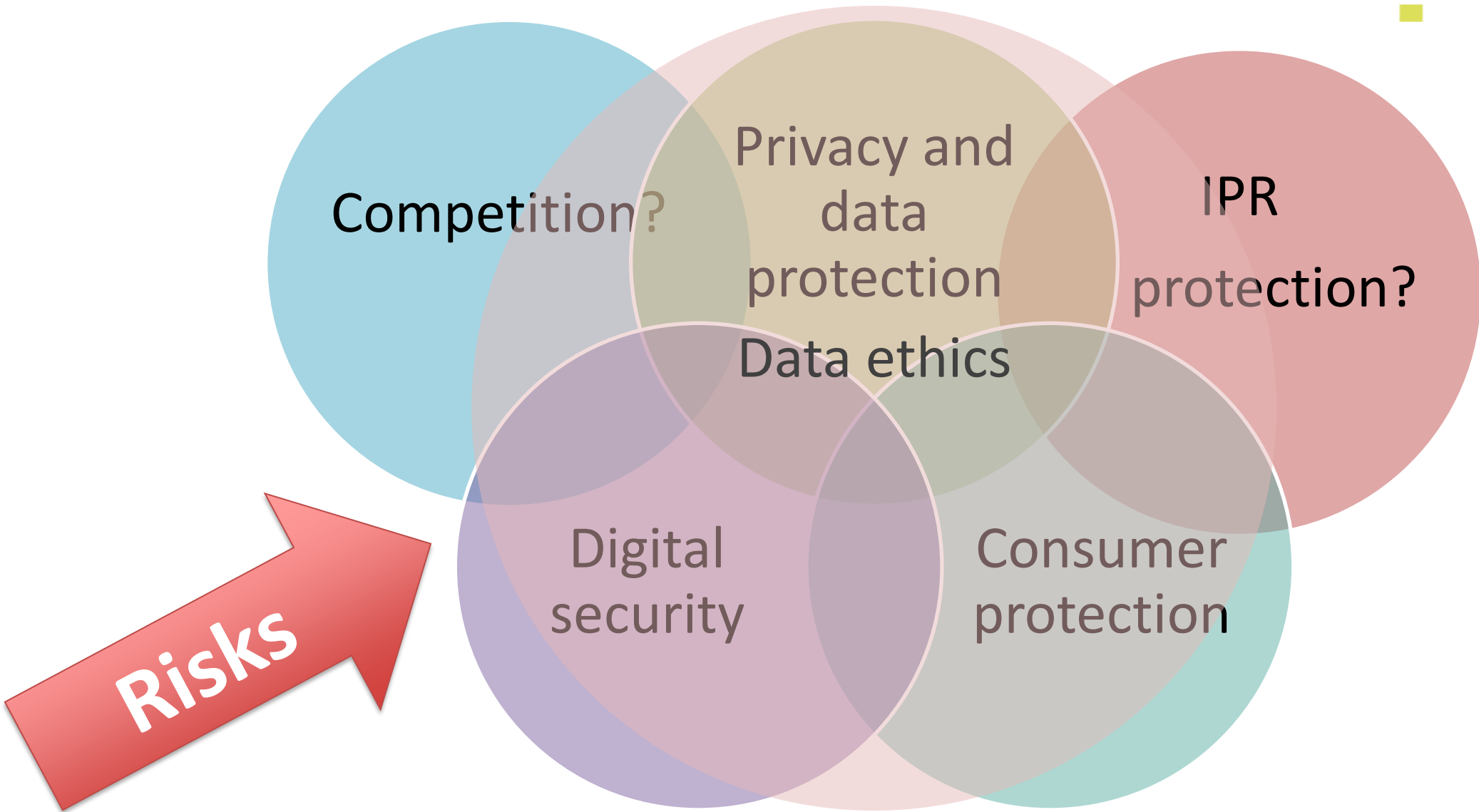
- Muitos governos estão adotando medidas sem precedentes para rastrear, monitorar e conter a disseminação do novo coronavírus (COVID-19), recorrendo a tecnologias digitais e estratégias de análises avançadas para coletar, processar e compartilhar dados para obter respostas eficazes na linha de frente.
- Embora as medidas excepcionais implementadas ou previstas em alguns países possam mostrar-se, finalmente, eficazes na limitação da propagação do vírus, algumas abordagens têm se mostrado controversas em termos de risco de violação de privacidade e outros direitos fundamentais dos cidadãos, especialmente quando essas medidas carecem de transparência ou não são objeto de ampla consulta à população.
- As autoridades responsáveis pela aplicação das normas sobre privacidade geralmente endossam uma abordagem pragmática e contextual em momentos de crise ou estado de emergência, e exercem um poder discricionário, de modo que o respeito aos princípios fundamentais de proteção de dados e privacidade não impeça respostas à COVID-19 que sejam necessárias e proporcionais na linha de frente.
- Os formuladores de políticas, em consulta com as autoridades nacionais de proteção de dados, devem avaliar as potenciais soluções de compromisso em matéria de utilização de dados durante esta crise (que equilibre riscos e benefícios), mas devem garantir que quaisquer medidas extraordinárias sejam proporcionais aos riscos e sejam implementadas com total transparência, responsabilidade e compromisso de cessar ou reverter imediatamente usos excepcionais de dados quando a crise terminar.



TACKLING CORONAVIRUS (COVID-19)  
CONTRIBUTING TO A GLOBAL EFFORT



# Trust in the digital economy as approached by the OECD



# Structure and narrative of this presentation



Data openness leads to a loss of control over data that increases the risks of violations of rights and other interests, which in turn can undermine trust in the data ecosystem

Some restrictions to data openness can be necessary to better control the risks of data openness to reinforce trust in the data ecosystem

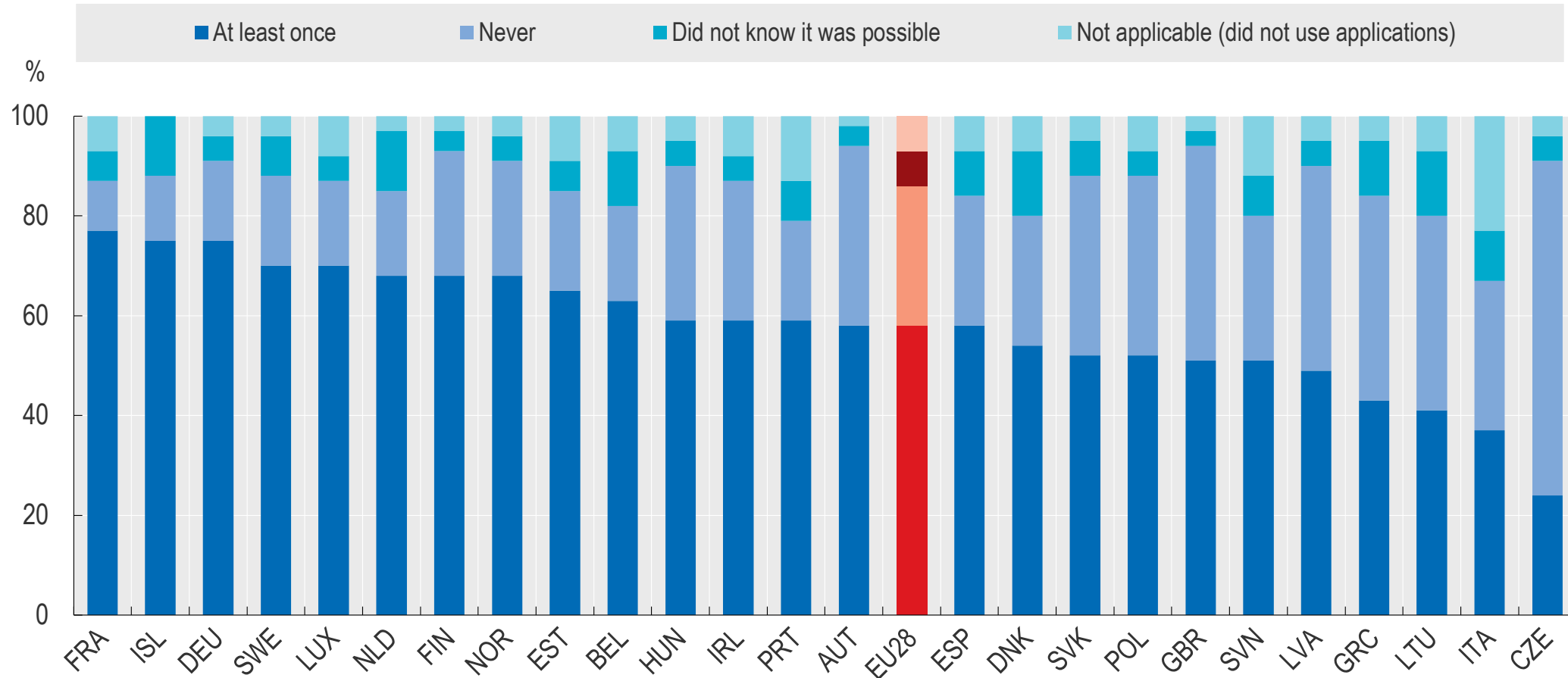
The need for more balanced risk-based approaches to data stewardship and control to enhance the trustworthiness of the data ecosystem

# THE RISKS OF DATA OPENNESS

---

# The willingness to share data varies considerably across countries

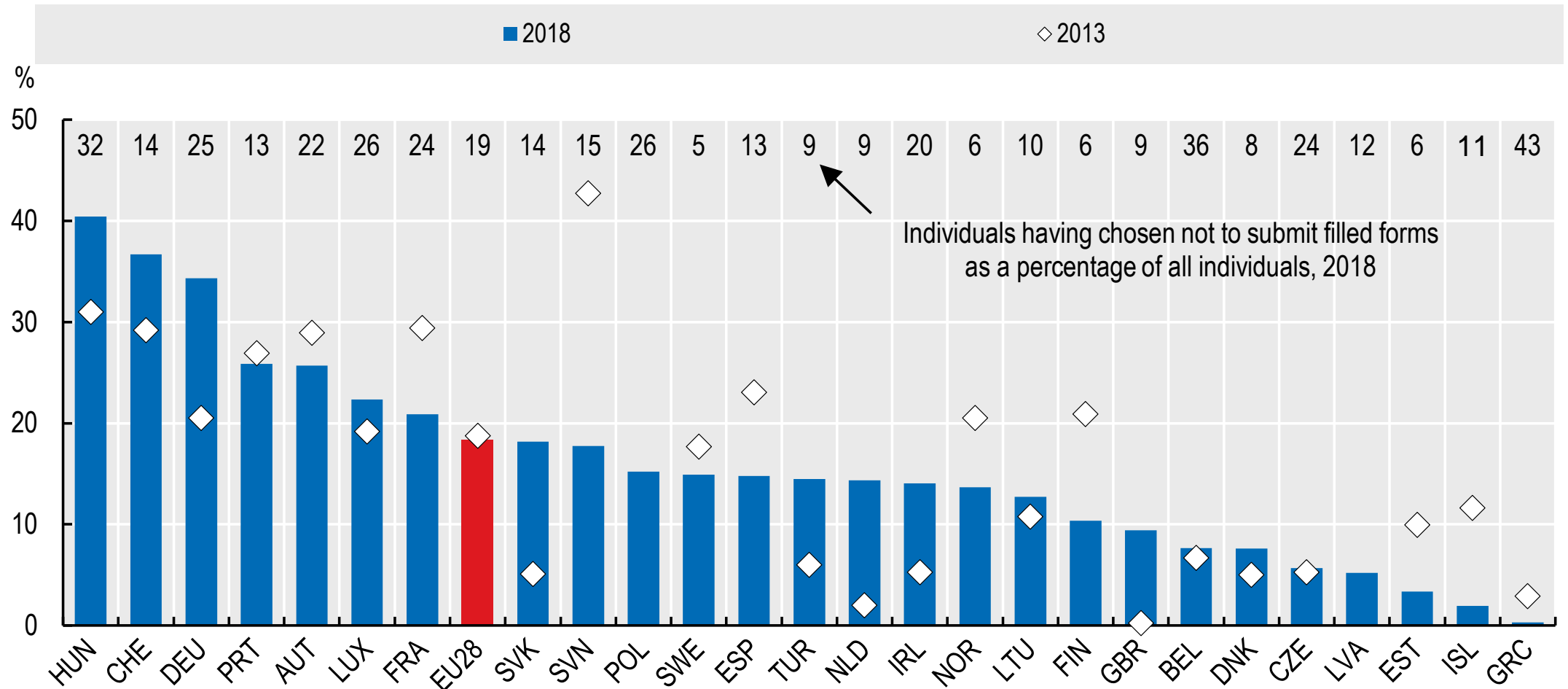
Individuals who restricted or refused access to their personal data when using or installing an app on a smartphone, 2018  
As a percentage of individuals using a smartphone for private purposes



OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, <https://doi.org/10.1787/62ff8236-en>, based on Eurostat Digital Economy and Society Statistics.

# Privacy and security concerns are often highlighted as a major cause for not using digital services

Individuals who did not submit official forms online due to privacy and security concerns, 2018  
As a percentage of individuals having chosen not to submit official forms online

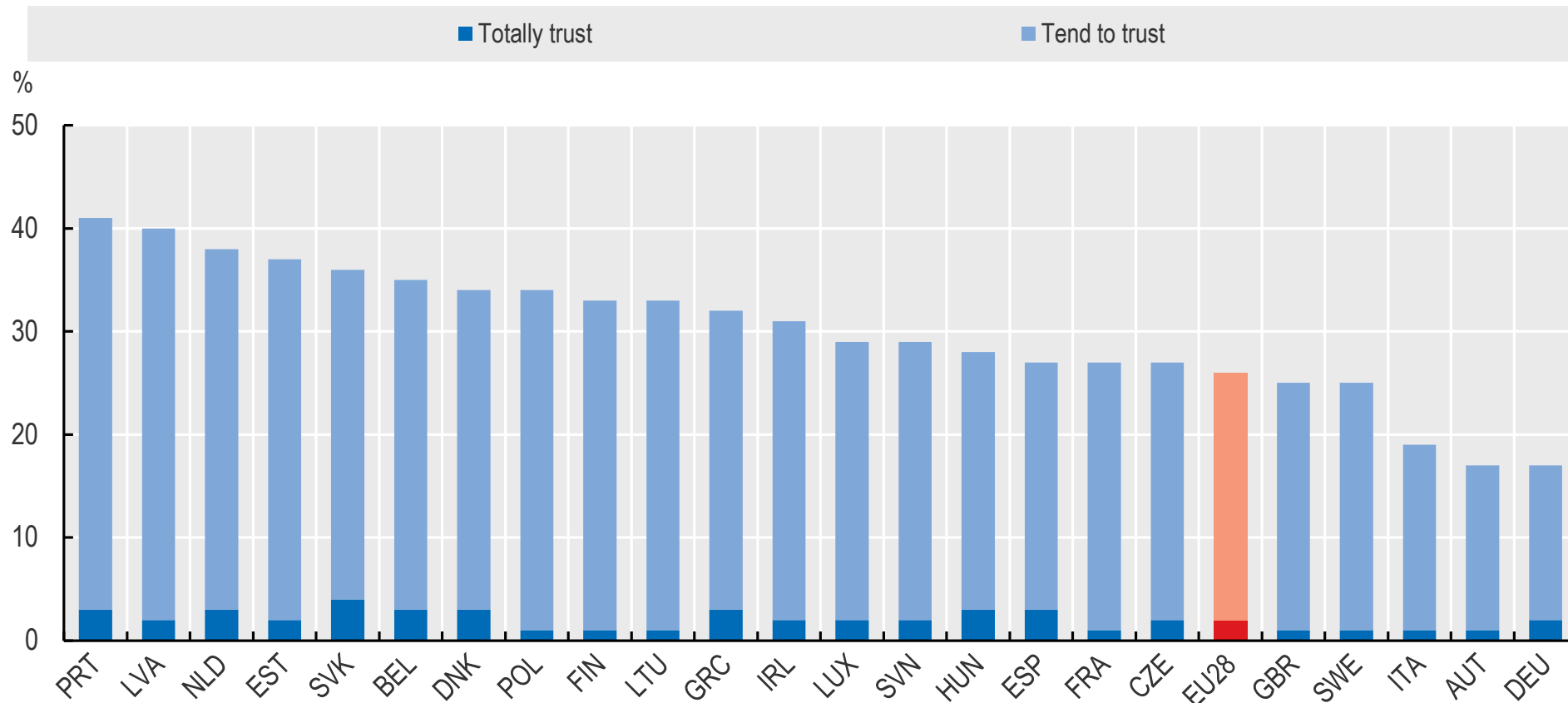


OECD (2019), *Measuring the Digital Transformation*, OECD Publishing, Paris, <https://doi.org/10.1787/86a789d9-en>, based on Eurostat, Digital Economy and Society Statistics, Comprehensive Database. For Switzerland, data refer to 2014 and 2017.



# The level of trust in digital services vary considerably across countries

Trust in information accessed through online social networks and messaging applications, 2018  
Percentage of respondents, "How much do you trust or not the news and information you access through online social networks and messaging apps?"



Other response items are the following : "Tend not to trust", "Do not trust at all" and "Don't know".

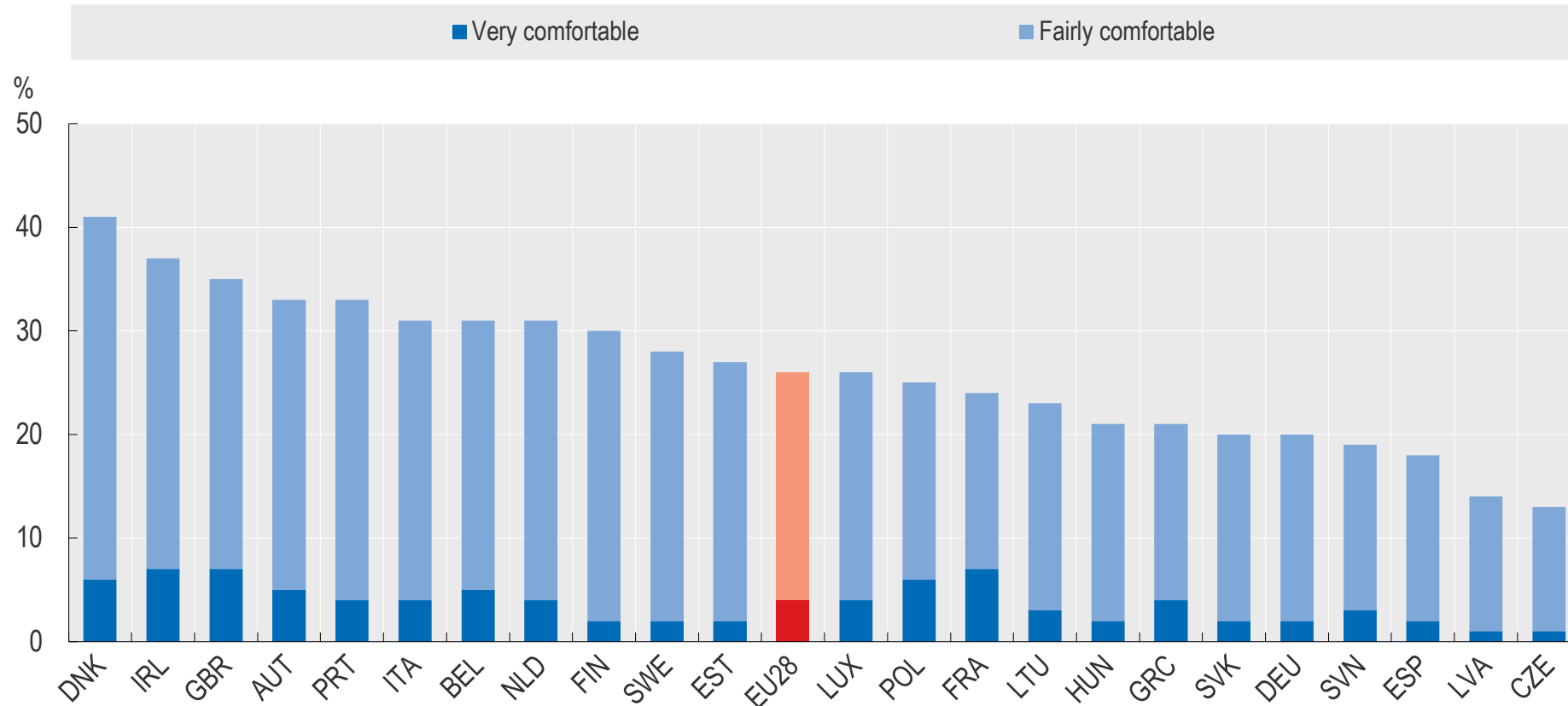
EC (2018), Fake news and disinformation online, Flash Eurobarometer, No. 464, April, Brussels.

<https://doi.org/10.1787/888933931390>

# The level of trust in digital services vary considerably across countries

## Attitudes towards online advertising on social media, 2016

Percentage of respondents, "To what extent are you comfortable or not with the fact that online social networks use information about your online activity and personal data to tailor advertisements or content to what interests you?"

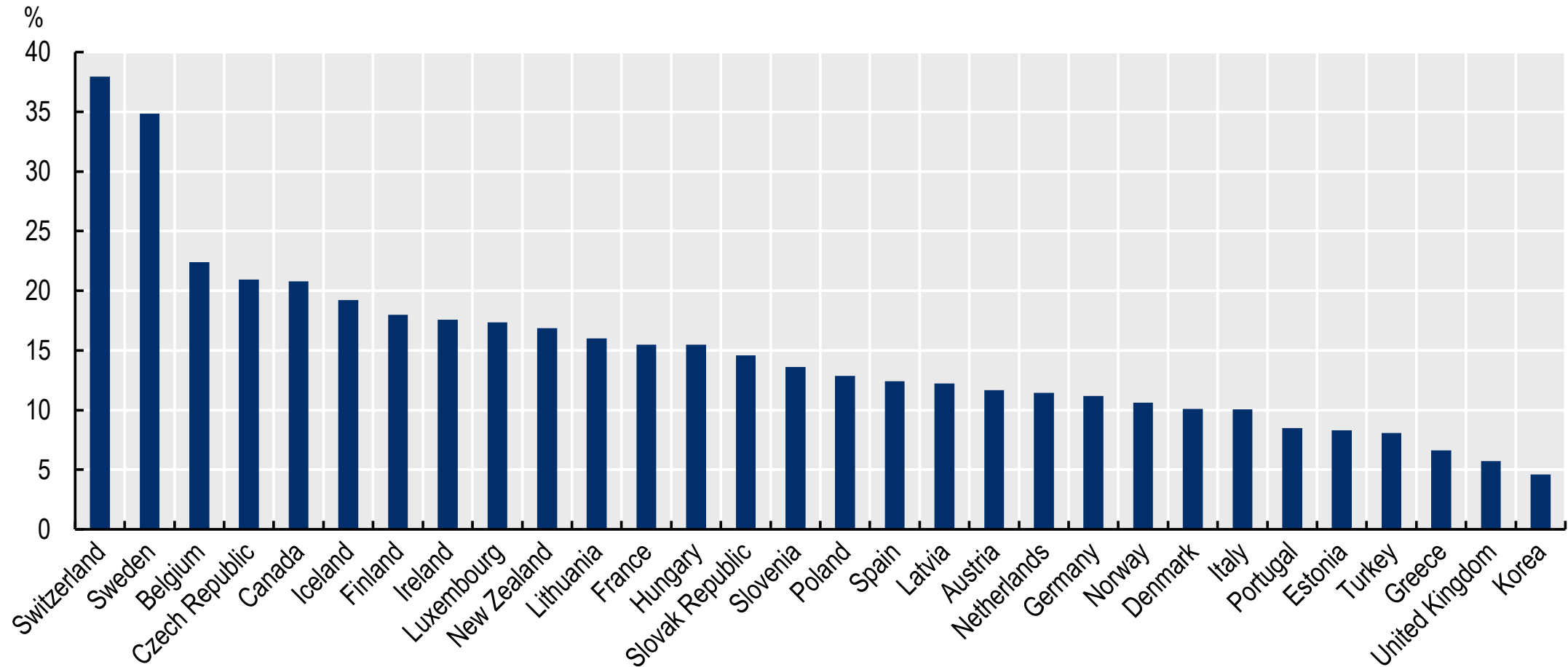


Other response items are the following : "Very uncomfortable", "Fairly uncomfortable", "Do not use the Internet", "Do not use online platforms" and "Don't know".

EC (2016), Online platforms, Special Eurobarometer, No. 447, June, Brussels. <https://doi.org/10.1787/888933931371>

# Digital security breaches also vary considerably across countries ...

Prevalence of security breaches in enterprises, 2019  
As a percentage of total firms with 10 or more employees



OECD (2021), OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, <https://doi.org/10.1787/64afab08-en>, based on OECD ICT Access and Usage by Businesses database, <http://oe.cd/bus>.

## ... and by sector

### Prevalence and type of digital security incidents by industry, 2019 Number of incidents and as a share of total incidents (%)

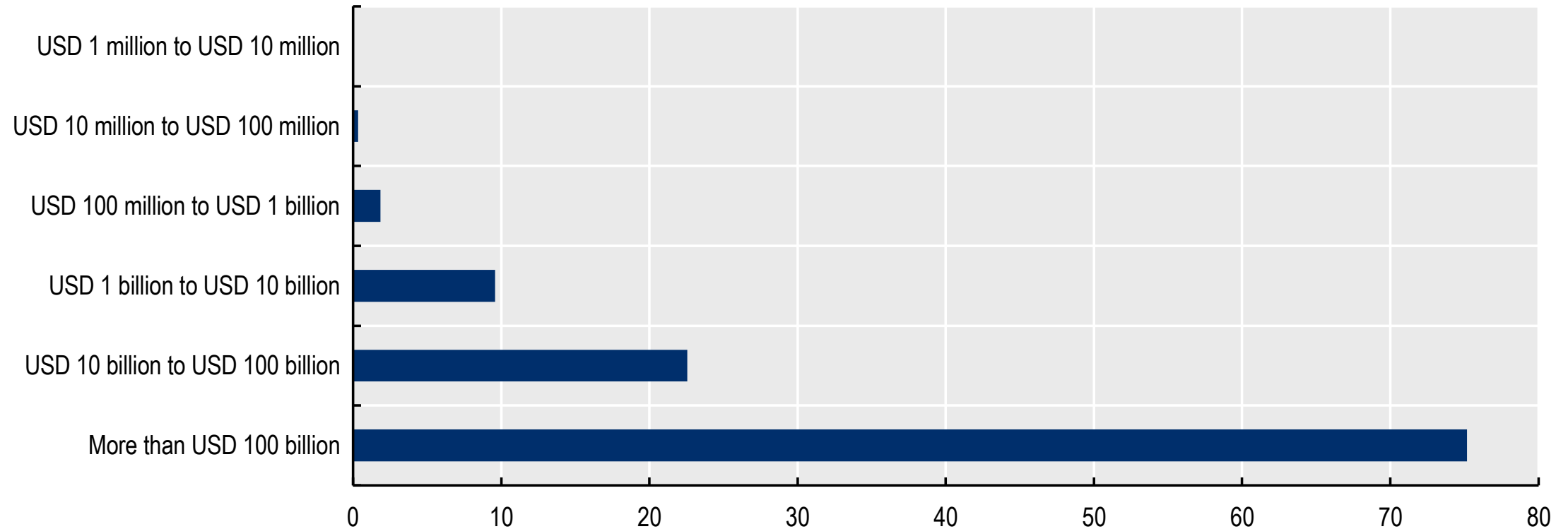
	Digital intensity	Prevalence of digital security risks		Actors (%)	Main data compromised (%)					
		Incidents	Breaches	External attacks	Personal data	Credentials	Internal data	Payment data	Bank data	Medical data
Professional, Scientific and Technical Services	High	7 463	326	75%	75%	45%				
Public Administration	Medium-high	6 843	346	59%	51%	33%				
Information services	High	5 741	360	67%	69%	41%	16%			
Financial and Insurance	High	1 509	448	64%	77%	35%			32%	
Manufacturing	Medium-low to high	922	381	75%	49%	55%		20%		
Educational Services	Medium-low	819	228	67%	75%	30%	13%			
Healthcare	Medium-low	798	521	51%	77%	18%				67%
Retail	Medium-high	287	146	75%	49%	27%		47%		
Arts, Entertainment and Recreation	Medium-high	194	98	67%	84%			25%		31%
Mining, extraction and utilities	Low	194	43	75%	41%	41%	19%			
Accommodation and food	Low	125	92	79%	44%	14%		68%		
Transportation and storage	Low	112	67	68%	64%	34%				
Other Services	Low to high	107	66	68%	81%	36%				
Construction	Low	37	25	95%	N/A	N/A				
Real Estate	Low	37	33	73%	83%	40%	43%			

Note: Digital intensity corresponds to a taxonomy of digital intensive sectors that accounts for some of the key facets of the digital transformation. The indicators used to classify 36 sectors defined along the international standard industrial classification of economic activities (ISIC revision 4) over the period 2013-15 are: share of ICT tangible and intangible (i.e. software) investment; share of purchases of intermediate ICT goods and services; stock of robots per hundreds of employees; share of ICT specialists in total employment; and the share of turnover from online sales.

Source: OECD (2021), OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, based on (Verizon, 2020; Calvino et al., 2018).

# ... and by firm size as measured in revenues

Annual breach likelihood, by firm revenue, United States, 2009-19

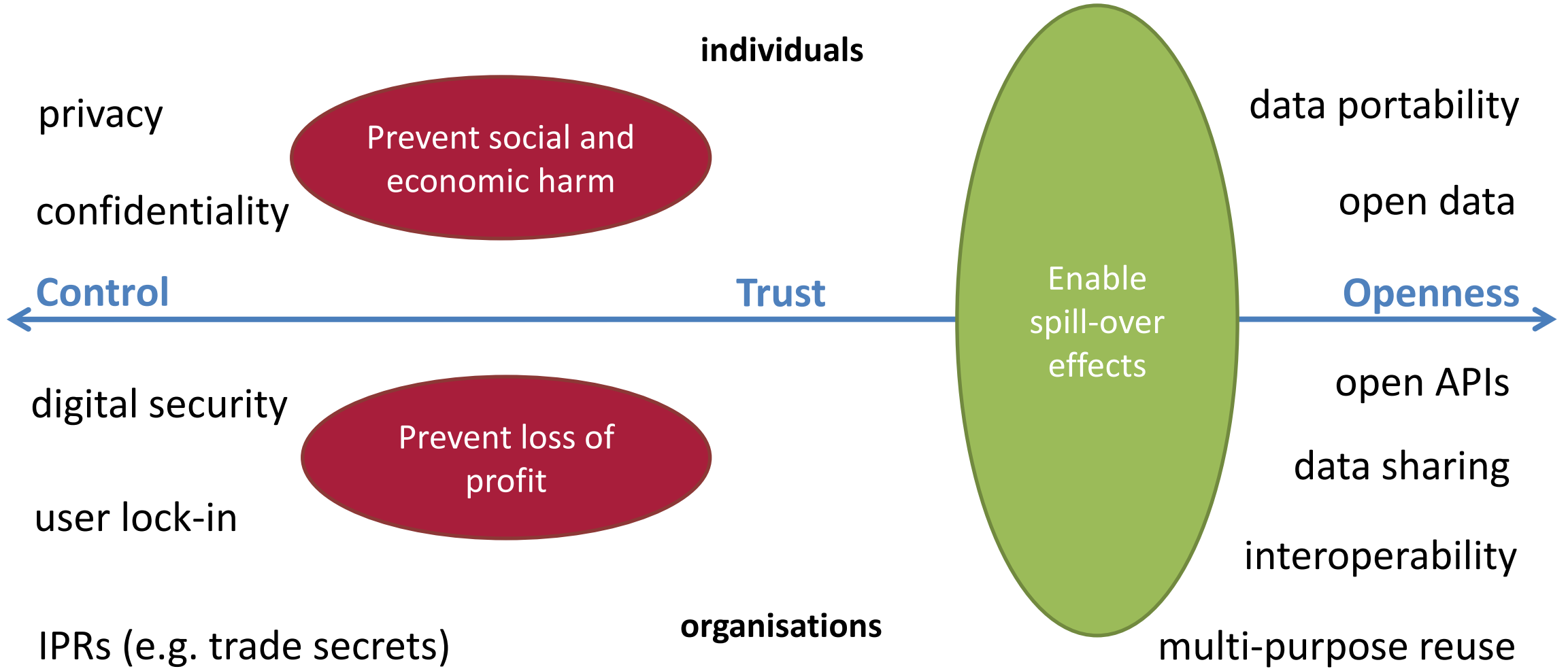


Cyentia Institute (2019), based on Advisen's Cyber Loss Data that tracks several different types of cyber events such as ransomware, privacy, denial of service, etc. They compile information from publicly-available sources such as breach disclosures, company filings, litigation details, Freedom of Information Act requests, etc., in a dataset that is periodically updated. The ten-year observation period from 2009-2019 includes 56 000 cyber events, of which 1 900 record financial losses associated with the event and nearly 12 000 have counts for the number of records involved.

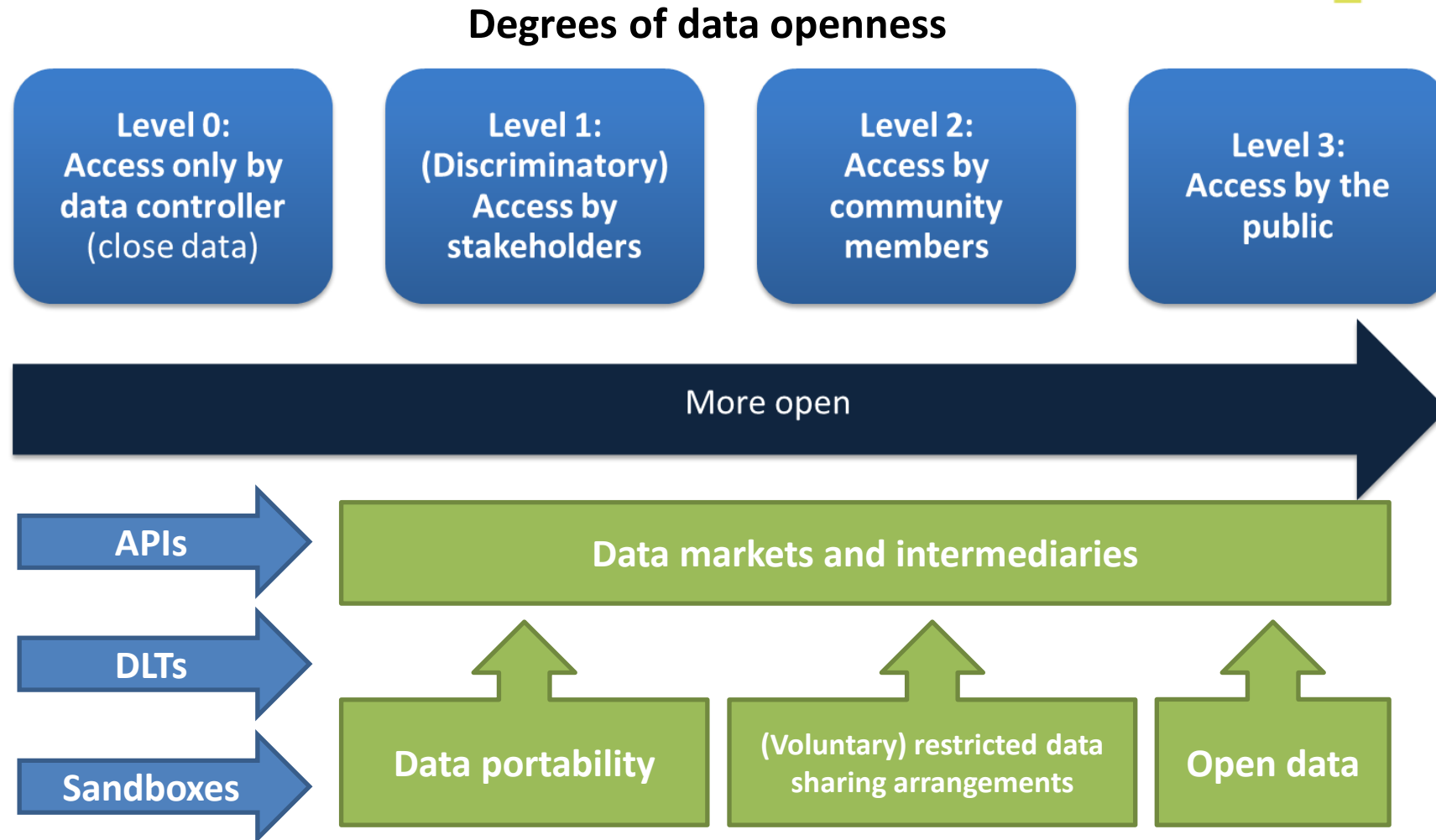
# THE TENSION BETWEEN DATA OPENNESS AND CONTROL

---

# Key dilemma : Striking the right balance between “openness” and “control”



# Data openness is not a binary concept but covers a continuum of degrees of openness which can be adjusted depending on the level of trust-worthiness

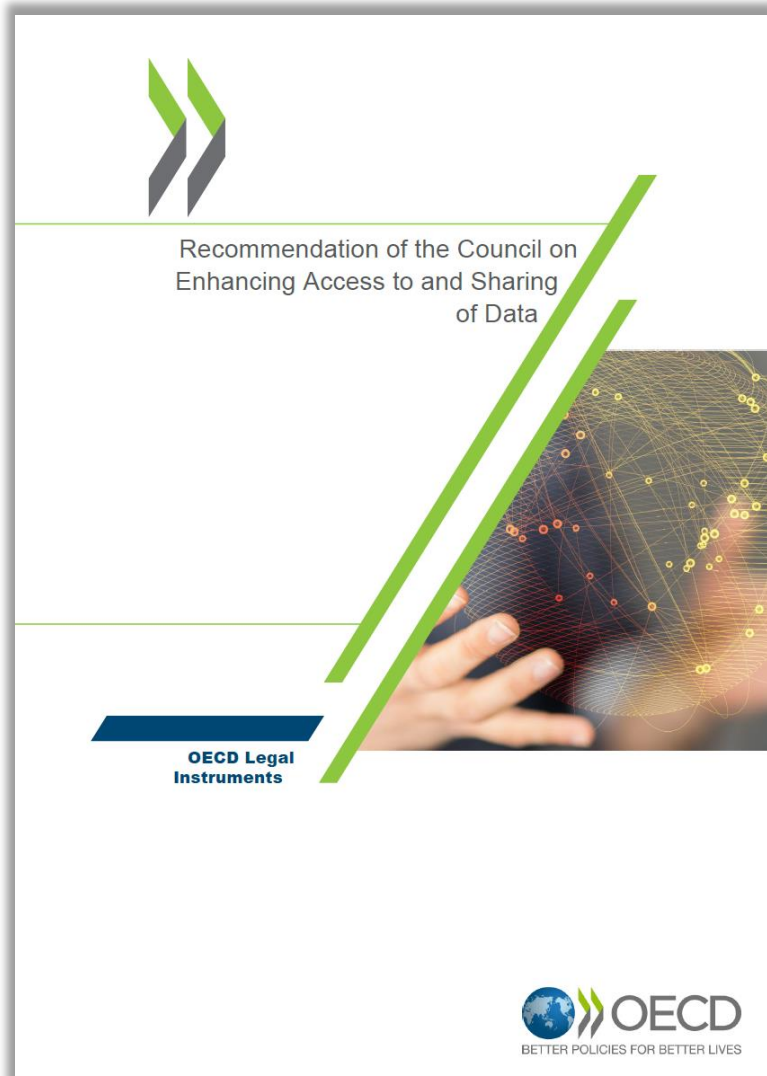




# THE OECD COUNCIL RECOMMENDATION ON EASD

---

# OECD member countries agreed this year to general principles for data access and sharing



## Objectives of the EASD Recommendation:

- Fostering the coherence of data governance frameworks across sectors and jurisdictions,
- Facilitating data access and sharing across sectors and jurisdictions,
- Enabling collaboration and the innovative re-use of data for growth and well-being,
- While protecting the rights of stakeholders and enhancing the trustworthiness of the data ecosystem.

Adhered by all OECD Members plus Brazil.

➤ Full text: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>

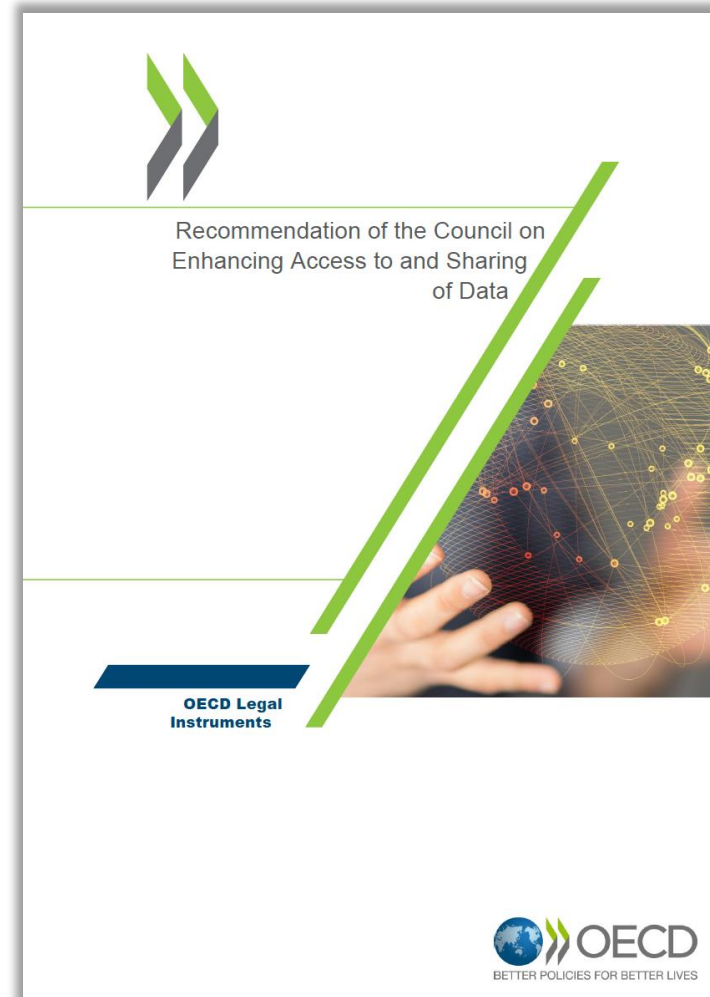
# The Council Recommendation on EASD provides a common foundation, and complements, existing guidance on data governance across the OECD

## Digital economy

- 2013 Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [[OECD/LEGAL/0188](#)]
- 2008 Council Recommendation for Enhanced Access and More Effective Use of Public Sector Information [[OECD/LEGAL/0362](#)]

## Science & technology

- 2021 Council Recommendation concerning Access to Research Data from Public Funding [[OECD/LEGAL/0347](#)]



## Digital government

- 2014 Council Recommendation on Digital Government Strategies [[OECD/LEGAL/0406](#)]

## Health data

- 2016 Council Recommendation on Health Data Governance [[OECD/LEGAL/0433](#)]

# Key provisions of the Council Recommendation on EASD

## Section 1. Reinforcing trust across the data ecosystem



III Empowerment and pro-active engagement



IV Strategic whole-of-government approach



V Maximising benefits while protecting rights and promoting a culture of responsibility

## Section 2. Stimulating investment in data and incentivising data access and sharing



VI Coherent incentives and sustainable business models and markets

## Section 3. Fostering effective and responsible data access, sharing, and use across society



VII Improving conditions for cross-border data access and sharing



VIII Findability, accessibility, interoperability and reusability of data across organisations



IX Capacity building for effective use of data

## III Empowerment and pro-active engagement

**III.RECOMMENDS** that [Adherents] **empower and pro-actively engage all relevant stakeholders alongside broader efforts to increase the trustworthiness of the data ecosystem** .... In particular, Adherents should:

- a) **Promote inclusive representation of and engage relevant stakeholders in the data ecosystem** – including vulnerable, underrepresented, or marginalised groups – in open and inclusive consultation processes during the design, implementation, and monitoring of data governance frameworks related to data access and sharing to reinforce trust;
- b) **Encourage competition-neutral data-sharing partnerships, including Public-Private Partnerships (PPPs)**, where data sharing across and between public and private sectors can create additional value for society. In so doing, Adherents should take all necessary steps to avoid conflicts of interest or undermining government open data arrangements or public interests;

...

### III Empowerment and pro-active engagement

**III.RECOMMENDS** that [Adherents] **empower and pro-actively engage all relevant stakeholders alongside broader efforts to increase the trustworthiness of the data ecosystem** .... In particular, Adherents should:

...

c) **Enhance transparency of data access and sharing arrangements to encourage the adoption of responsible data governance practices throughout the data value cycle** that meet applicable, recognised, and widely accepted technical, organisational, and legal standards and obligations, including codes of conduct, ethical principles and privacy and data protection regulation.

Where personal data is involved, Adherents should ensure transparency in line with privacy and data protection frameworks with respect to what personal data is accessed and shared, including with whom it is shared, for what purpose, and under what conditions access may be granted to third parties;

d) **Empower individuals, social groups, and organisations** through appropriate mechanisms and institutions such as trusted third parties that increase their agency and control over data they have contributed or that relate to them, and enable them to recognise and generate value from data responsibly and effectively.

## IV Strategic whole-of-government approach

**IV.RECOMMENDS** that Adherents **adopt a strategic whole-of-government approach to data access and sharing** to ensure that data access and sharing arrangements help effectively and efficiently meet specific societal, policy, and legal objectives that are in the public interest. In particular, Adherents should:

a) **Prioritise data access and sharing arrangements** that help achieve such objectives, taking into account applicable laws and regulations. In so doing, Adherents should work together with key stakeholders to clearly define the purpose of these arrangements and identify data relevant to these purposes, taking into account their benefits, costs, and possible risks;

b) **Adopt and regularly review coherent, flexible, and scalable data governance frameworks** – including national data strategies, which integrate cross-cutting economic, social, cultural, technical, and legal governance issues – in order to foster data access and sharing within and across society, public and private sectors, and jurisdictions;

...

## IV Strategic whole-of-government approach

**IV.RECOMMENDS** that Adherents **adopt a strategic whole-of-government approach to data access and sharing** to ensure that data access and sharing arrangements help effectively and efficiently meet specific societal, policy, and legal objectives that are in the public interest. In particular, Adherents should:

...

- c) **Demonstrate strong leadership**, ideally at the highest level of government, combined with a whole-of-government approach that enables effective policy coordination and implementation of these frameworks with multi-stakeholder participation; and
- d) **Adopt technology-neutral and agile legal and regulatory environments** that promote responsible data access and sharing and enable regulatory innovation, while providing the necessary legal certainty and protection with the engagement of all relevant independent enforcement authorities, oversight bodies, and stakeholder groups.



## V Maximising benefits while protecting rights and promoting a culture of responsibility

**V. RECOMMENDS** that Adherents **seek to maximise the benefits of [EASD measures], while protecting individuals' and organisations' rights and taking into account other legitimate interests and objectives, ....** In this regard, Adherents should:

**a) Encourage ... arrangements that ensure that data are as open as possible to maximise their benefits and as closed as necessary to protect legitimate public and private interests, including interests** related to national security, law enforcement, privacy and personal data protection, and IPRs as well as ethical values and norms such as fairness, human dignity, autonomy, self-determination, and the protection against undue bias and discrimination between individuals or social groups;

**b) Take necessary and proportionate steps to protect these legitimate public and private interests as a condition for data access and sharing.** In so doing, Adherents should strive to ensure that stakeholders are fully informed as to their rights (including their right to information and to obtain redress), responsibilities and respective liabilities in case of violations of privacy, IPRs, competition laws, or other rights and obligations;

...

## V Maximising benefits while protecting rights and promoting a culture of responsibility

**V. RECOMMENDS** that Adherents **seek to maximise the benefits of [EASD measures], while protecting individuals' and organisations' rights and taking into account other legitimate interests and objectives, ....** In this regard, Adherents should:

...

**c) Ensure that stakeholders are held accountable in taking responsibility, according to their roles, for the quality of the data they share and for the systematic implementation of risk management measures throughout the data value cycle, including [data security].** To this effect, Adherents should promote the adoption of impact assessments and audits as well as responsible stewardship ... within organisations, and appropriate human resource policies that clearly assign [roles and responsibilities] ...;

**d) Foster the adoption of conditioned data access and sharing arrangements with the use of technological and organisational environments and methods,** including data access control mechanisms and privacy enhancing technologies, through which data can be accessed and shared in a safe and secure way between approved users, combined with legally binding and enforceable obligations to protect [rights and interests];

## VII Improving conditions for cross-border data access and sharing

**VII.RECOMMENDS** that Adherents **further improve conditions for cross-border data access and sharing with trust**. To this effect, Adherents should:

- a) **Assess, and to the extent possible minimise, restrictions to cross-border data access and sharing**, in particular for purposes of global public interest, taking into account the need to ensure respect for fundamental rights and vital interests, including the protection of privacy and intellectual property rights and the right to access public information;
- b) **Ensure that measures that condition cross-border data access and sharing are non-discriminatory, transparent, necessary, and proportionate to the level of risk**, taking into account, among others, the sensitivity of the data, the purpose and context of data access, sharing, and use, and the extent to which measures are in place to enforce accountability irrespective of the jurisdiction in which the data is stored;
- c) **Promote continued dialogue and international co-operation on ways to foster data access and sharing across jurisdictions** – including through the implementation of trust-enhancing measures as set out above – as well as the interoperability and mutual recognition of data access and sharing arrangements, taking into account applicable legal requirements and global standards.

**IX. RECOMMENDS** that Adherents **adopt measures to enhance the capacity of all stakeholders to effectively use data responsibly along the data value cycle.** In particular, Adherents should:

**a) Foster awareness about the benefits and risks of data access, sharing, and use to encourage responsible data governance throughout the data value cycle** by engaging in dialogues with all relevant stakeholder groups and partnerships. To this effect, Adherents should disseminate good practices on data access, sharing, and use that help address barriers to accessing and sharing data responsibly and increase the capacity of individuals and organisations to manage, access, share, and use data responsibly;

**b) Promote the development of the data-related skills and competencies** needed, including by workers and public servants, to harness the benefits of data access, sharing, and use throughout the data value cycle in a manner consistent with the strategic approach to data access and sharing as set out above. This should include promoting data literacy ... and increasing citizen's capacity to understand relevant data governance issues and exert their rights;

...

# Selected background documents

- [Data-driven innovation for growth and well-being](#) (October 2015)
- [Health in the 21st Century: Putting Data to Work for Stronger Health Systems](#) (November 2019)
- [Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies](#) [Policy note] (November 2019)
- [The Path to Becoming a Data-Driven Public Sector](#) (November 2019)
- [A revised typology of risks for children in the digital environment](#) (January 2021)
- [Understanding the digital security of products: An in-depth analysis](#) [Policy brief] (February 2021)
- [Encouraging vulnerability treatment: Overview for policy makers](#) [Policy brief] (February 2021)

Find out more about our work at <https://goingdigital.oecd.org/>, [www.oecd.org/sti/ieconomy/privacy.htm](http://www.oecd.org/sti/ieconomy/privacy.htm), [www.oecd.org/sti/ieconomy/protecting-children-online.htm](http://www.oecd.org/sti/ieconomy/protecting-children-online.htm), [www.oecd.org/internet/ieconomy/enhanced-data-access.htm](http://www.oecd.org/internet/ieconomy/enhanced-data-access.htm), and [www.oecd.org/digital/ieconomy/digital-security/](http://www.oecd.org/digital/ieconomy/digital-security/)