2021 SUMMER SCHOOL
Towards a Digital Transformation & Innovation in Latin America
30 November 2021

SESSION 7: TRUST, PRIVACY AND SAFETY ONLINE

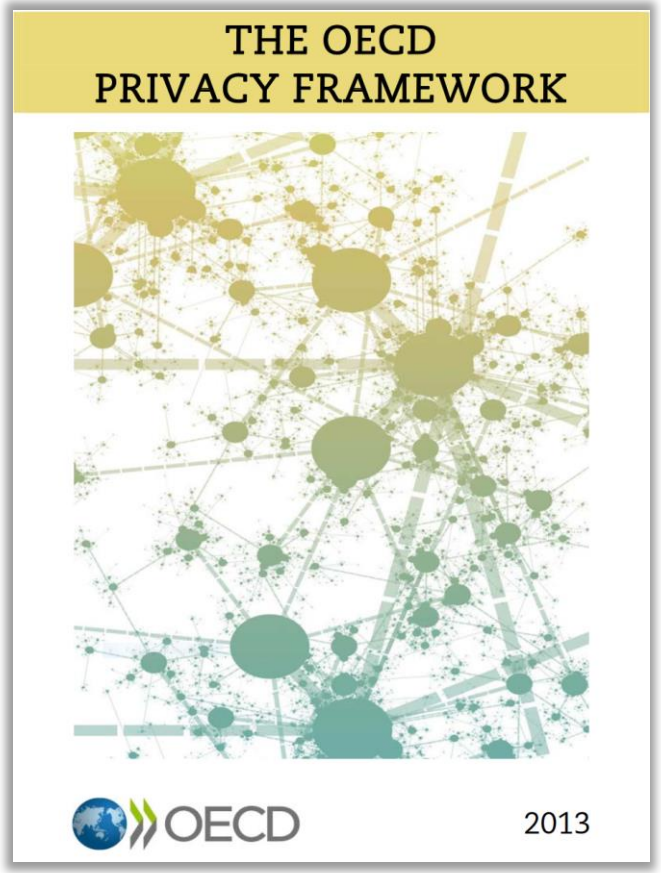
Focusing on the OECD Council Recommendation on Enhancing Access to and Sharing of Data

Christian.Reimsbach-Kounatze@oecd.org
Twitter: @chreko

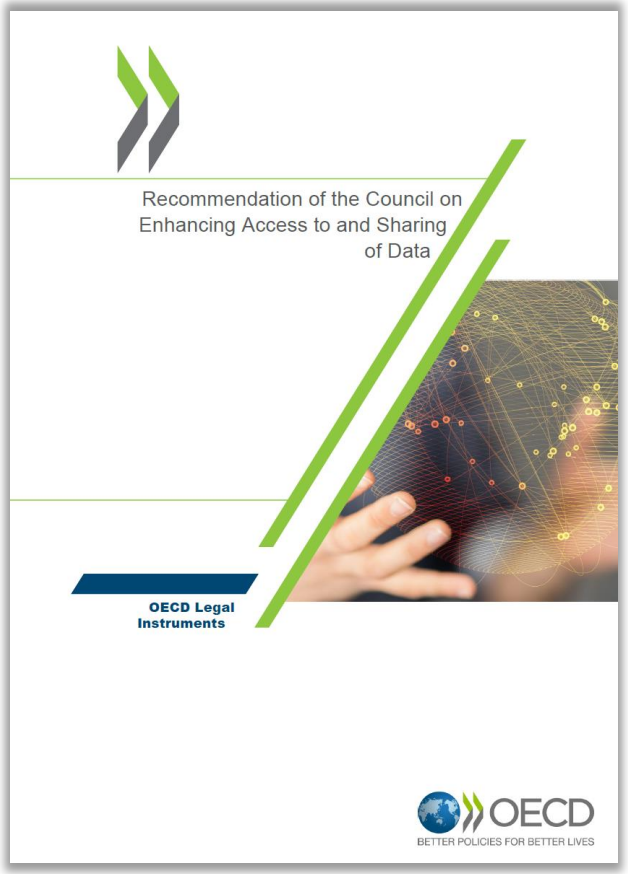
OECD
BETTER POLICIES FOR BETTER LIVES

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

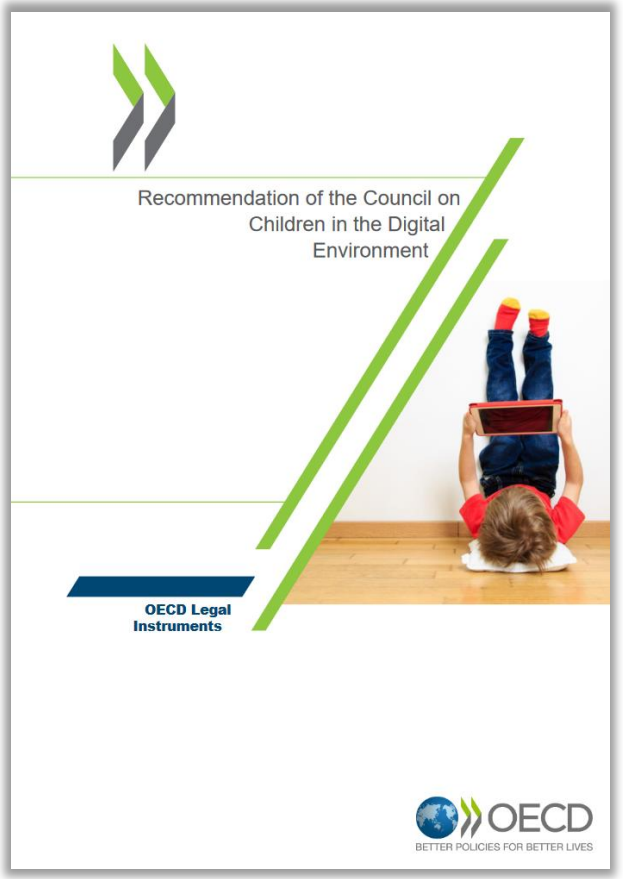
Three major areas of work covered by WPDGP



Privacy

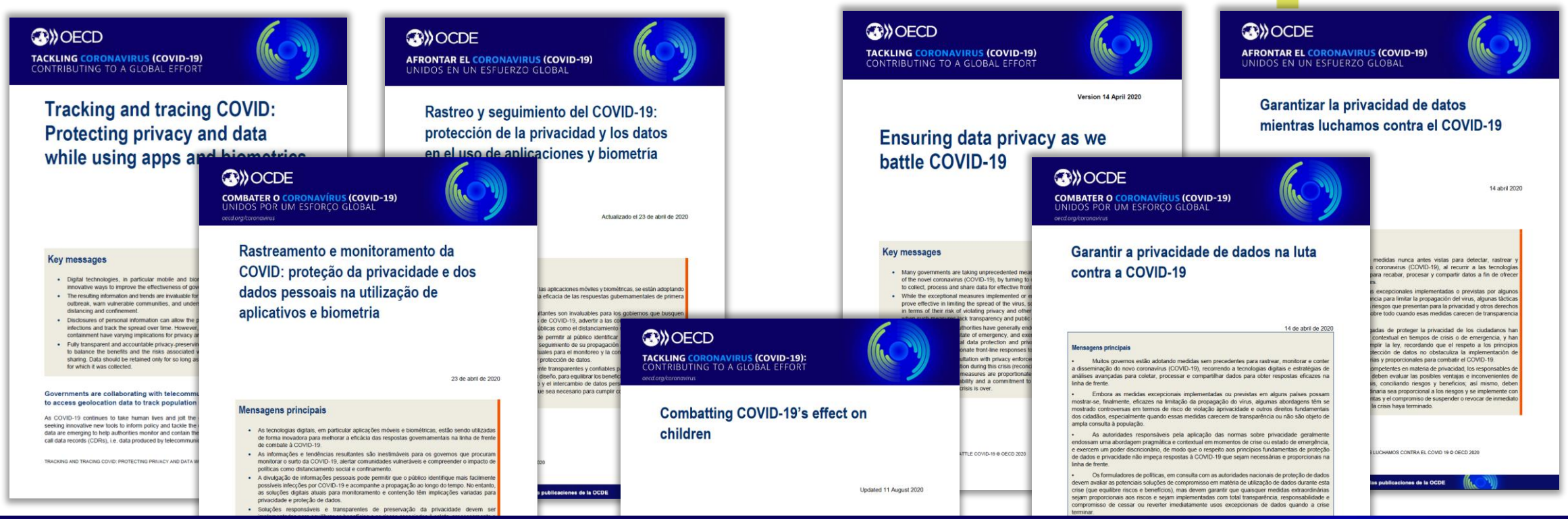


Data access & sharing



Children online

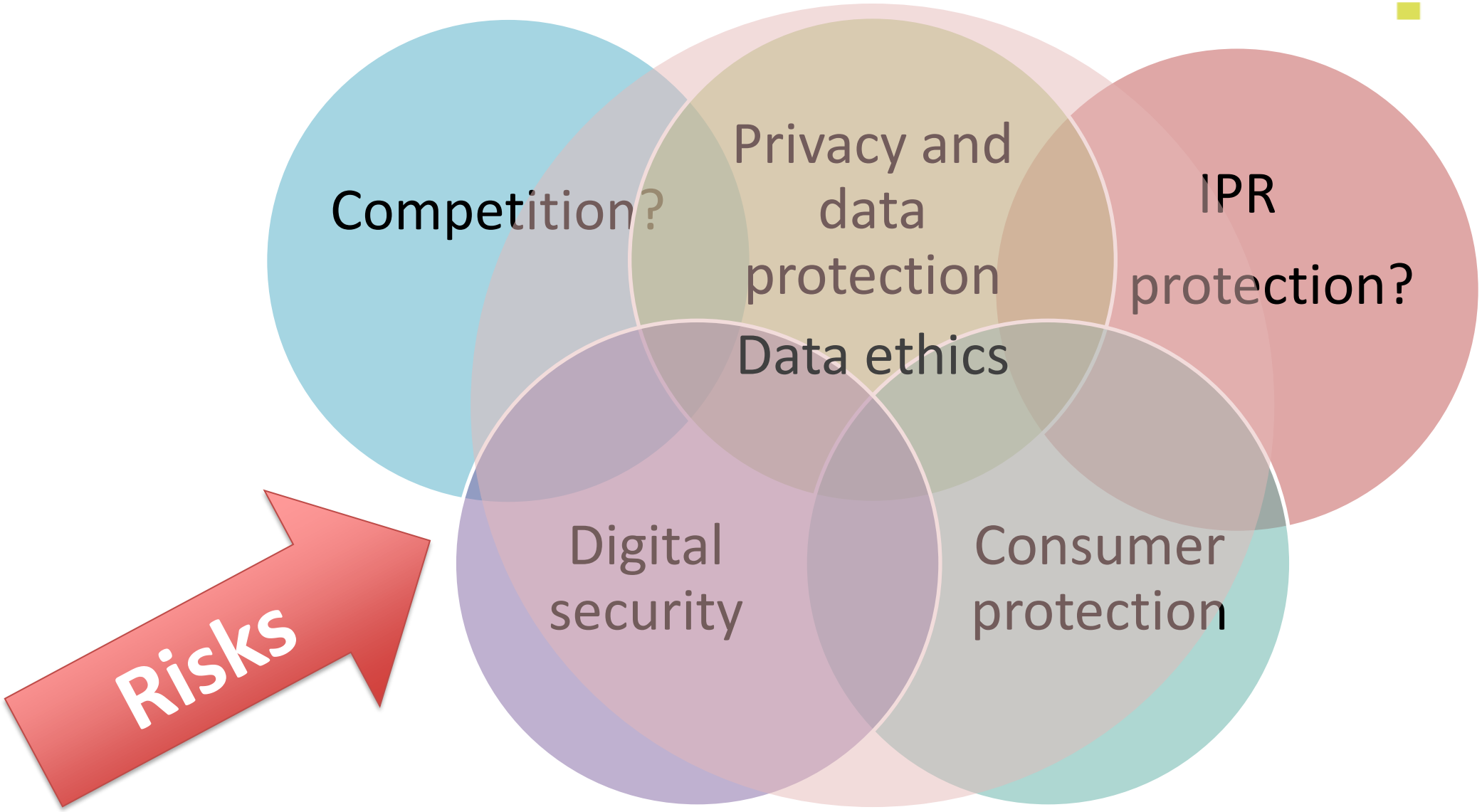
WPDGP work on data governance and privacy in the context of COVID-19



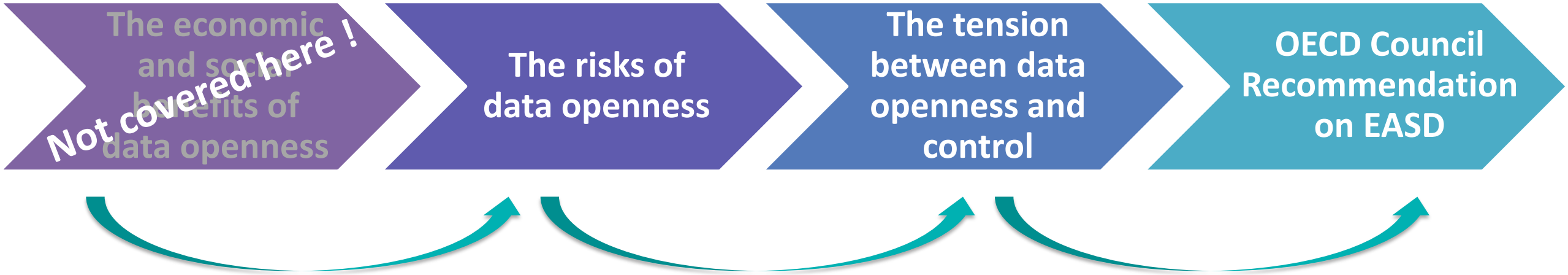
OECD

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

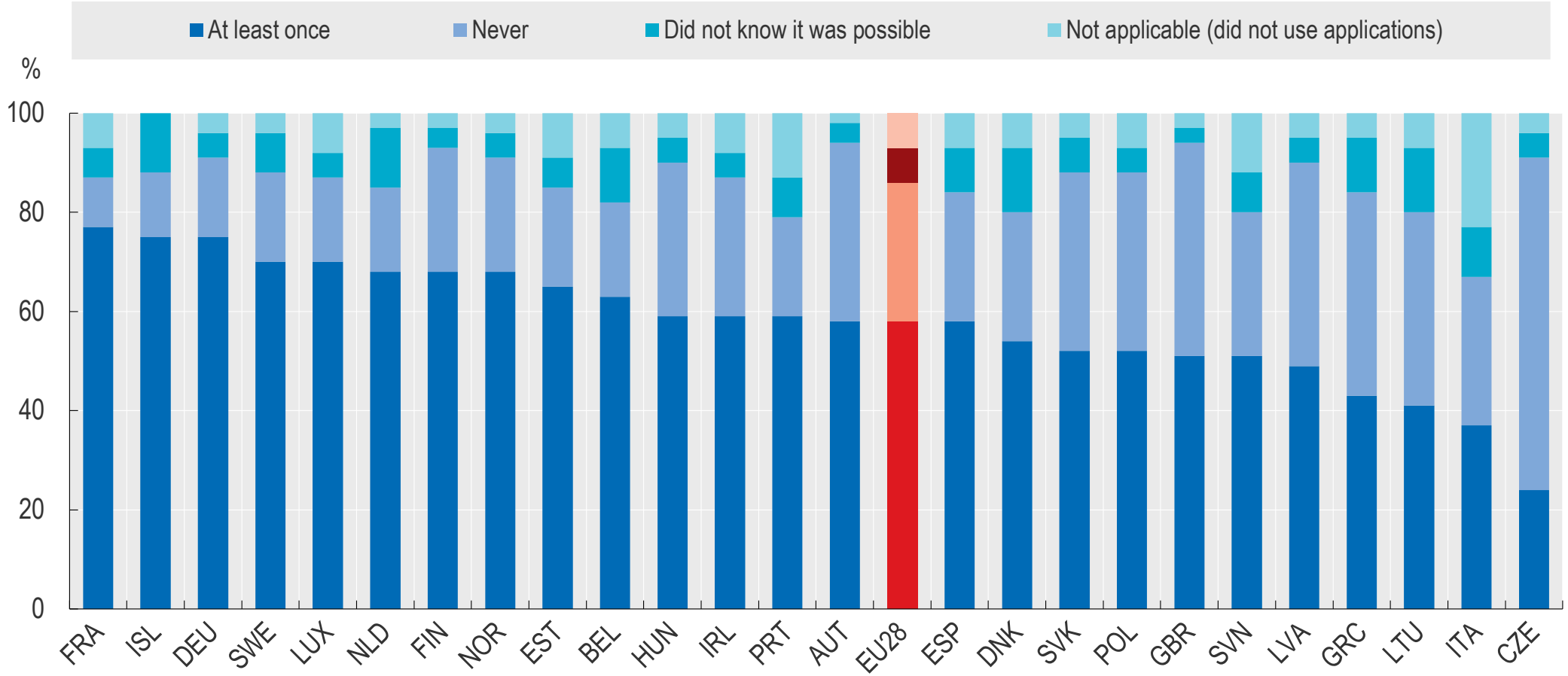
The need for more balanced risk-based approaches to data stewardship and control to enhance the trustworthiness of the data ecosystem

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

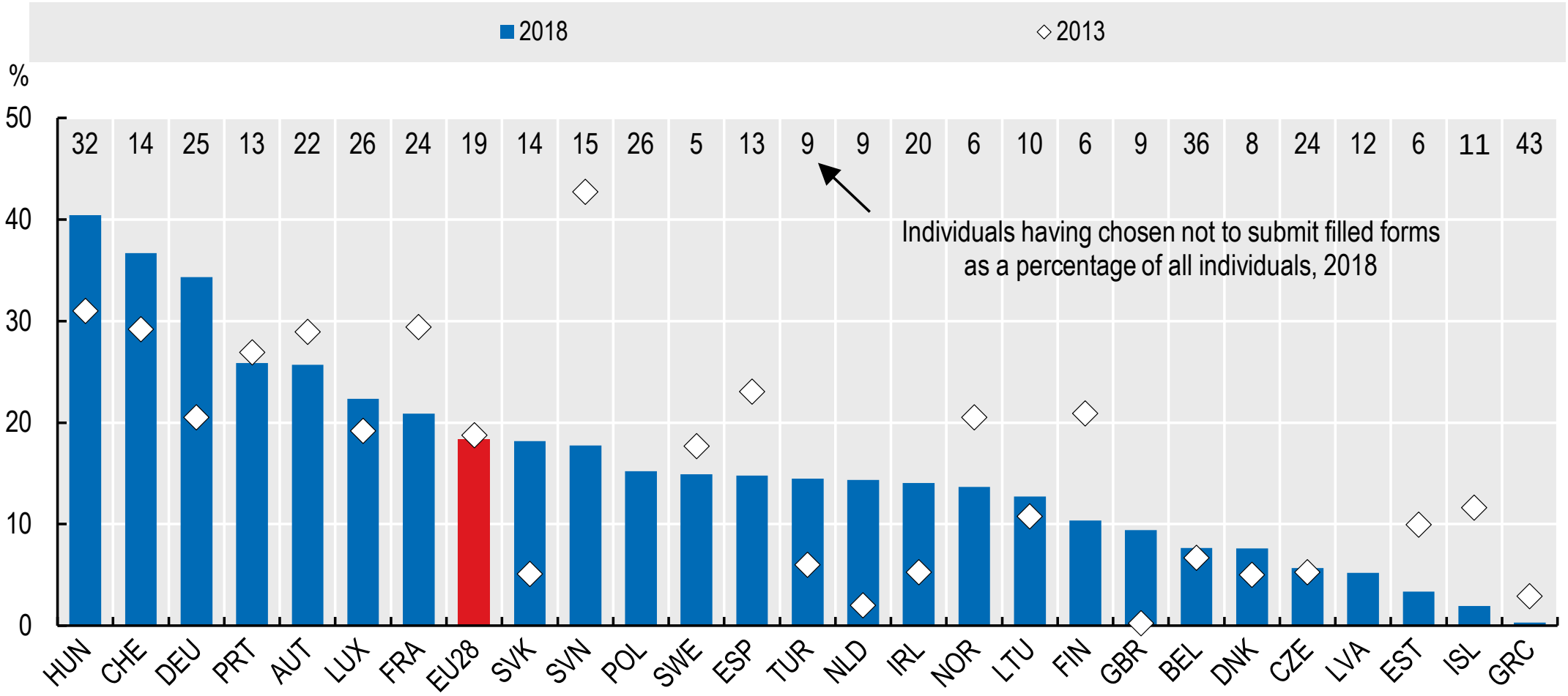


OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, https://doi.org/10.1787/62ff8236-en, based on Eurostat Digital Economy and Society Statistics.

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

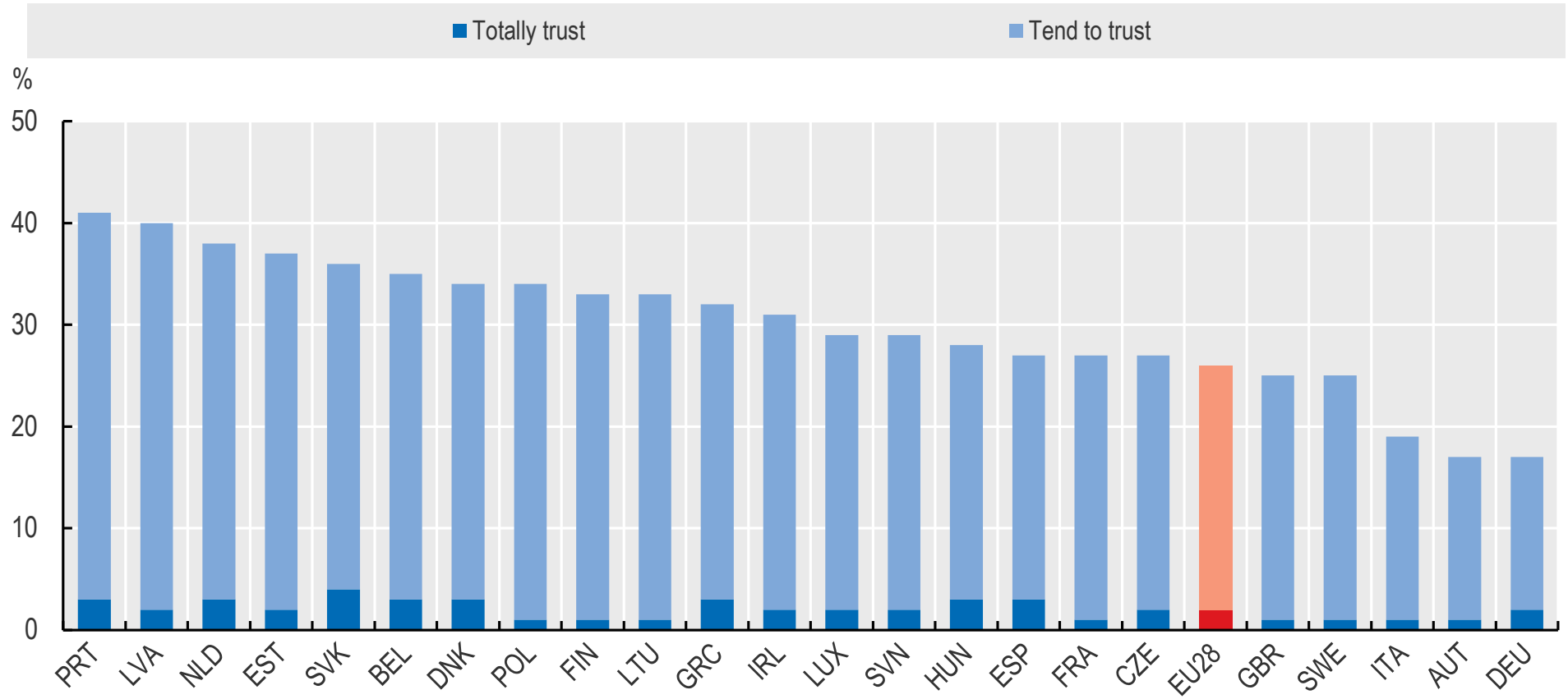


OECD (2019), *Measuring the Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/86a789d9-en, based on Eurostat, Digital Economy and Society Statistics, Comprehensive Database. For Switzerland, data refer to 2014 and 2017.

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".

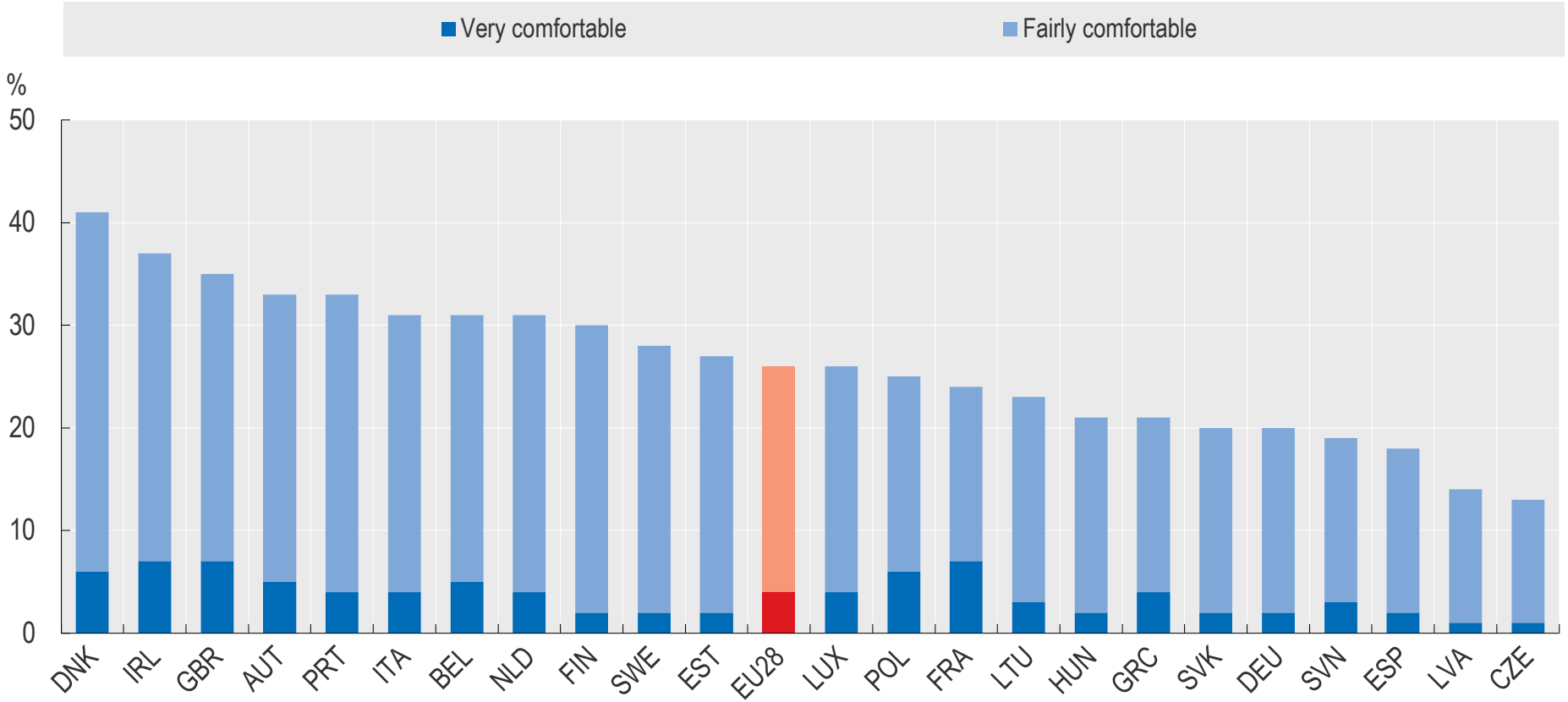
EC (2018), Fake news and disinformation online, Flash Eurobarometer, No. 464, April, Brussels.

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?”



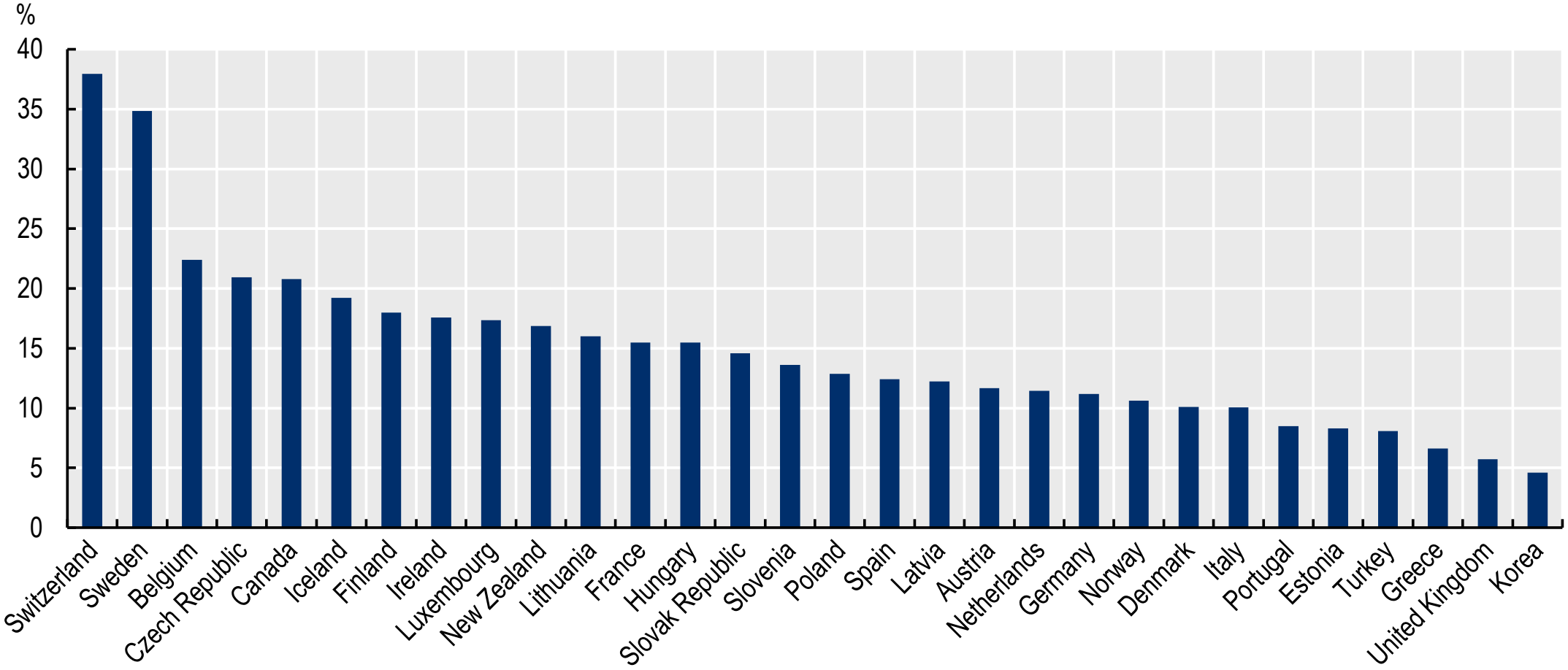
Other response items are the following : "Very uncomfortable", "Fairly uncomfortable", "Do not use the Internet", "Do not use online platforms" and "Don't know".

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

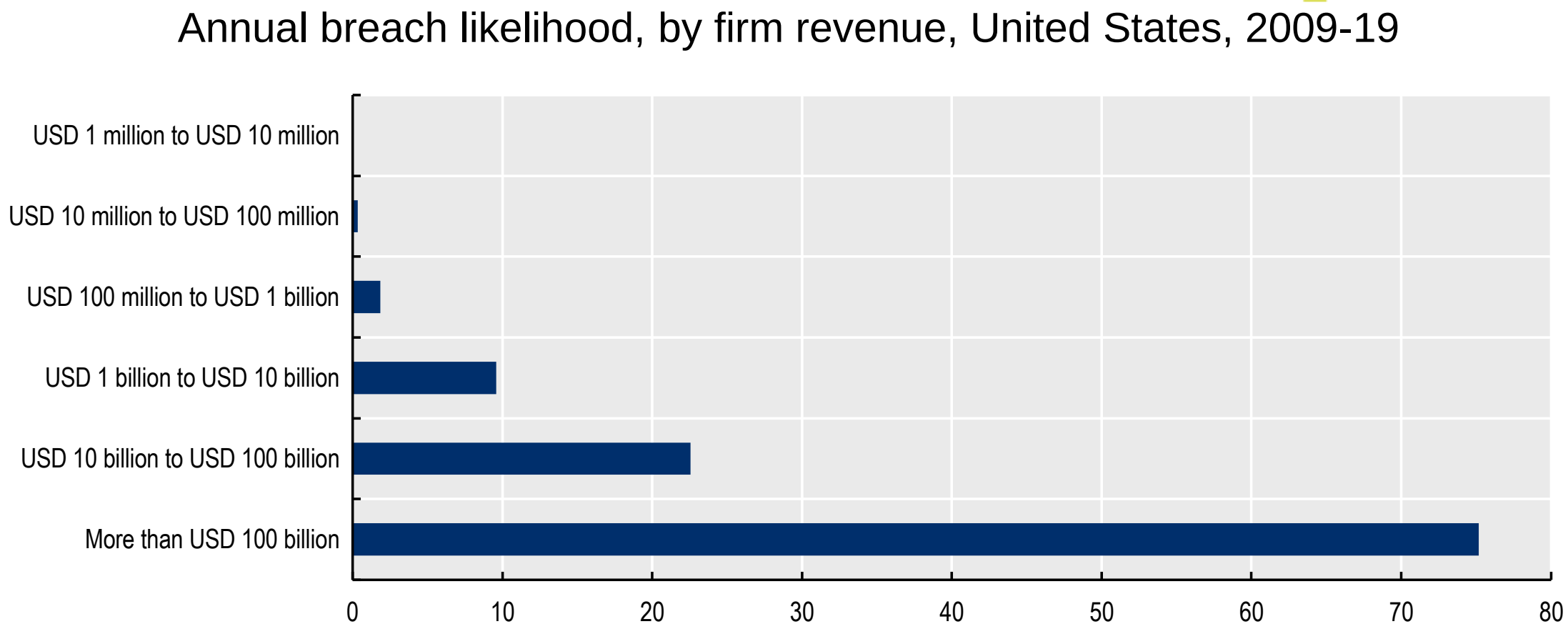
Prevalence and type of digital security incidents by industry, 2019
Number of incidents and as a share of total incidents (%)

	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).

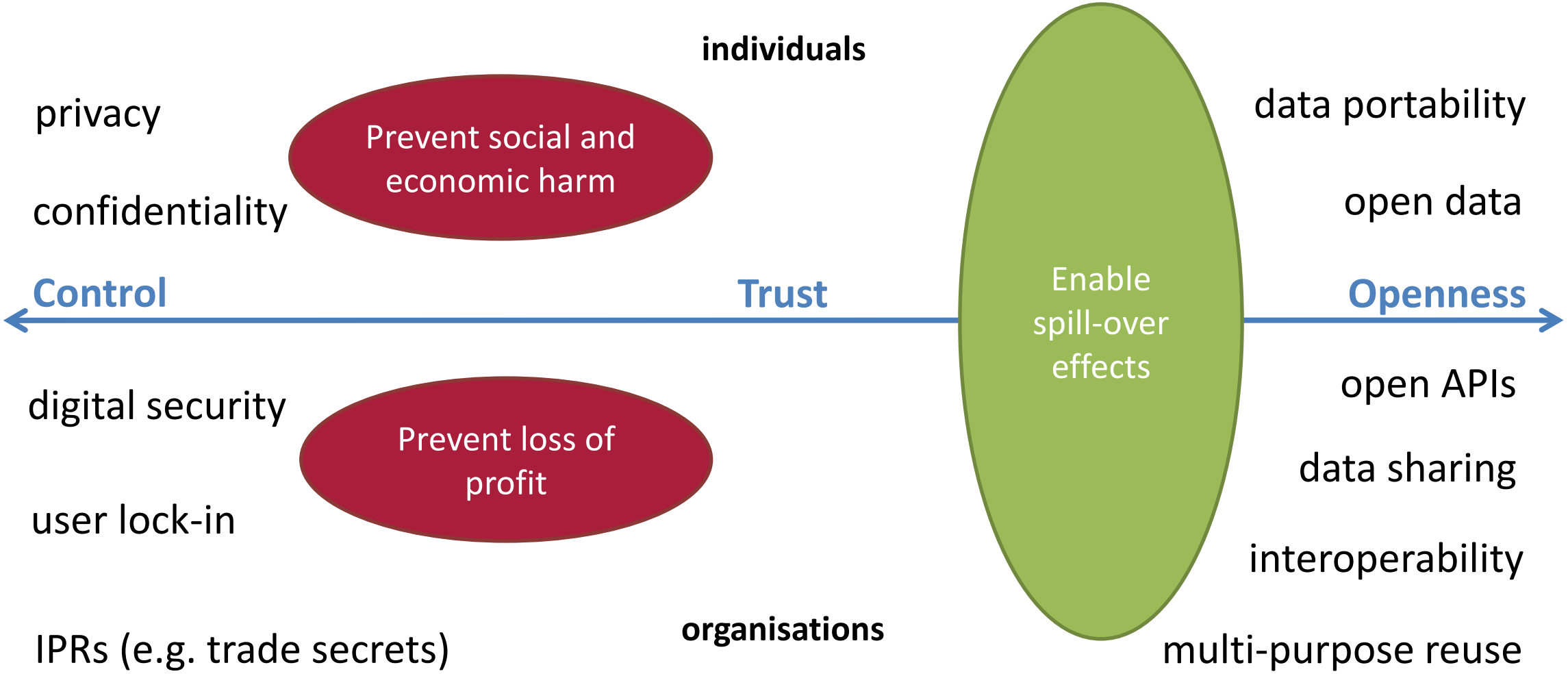
… and by firm size as measured in revenues



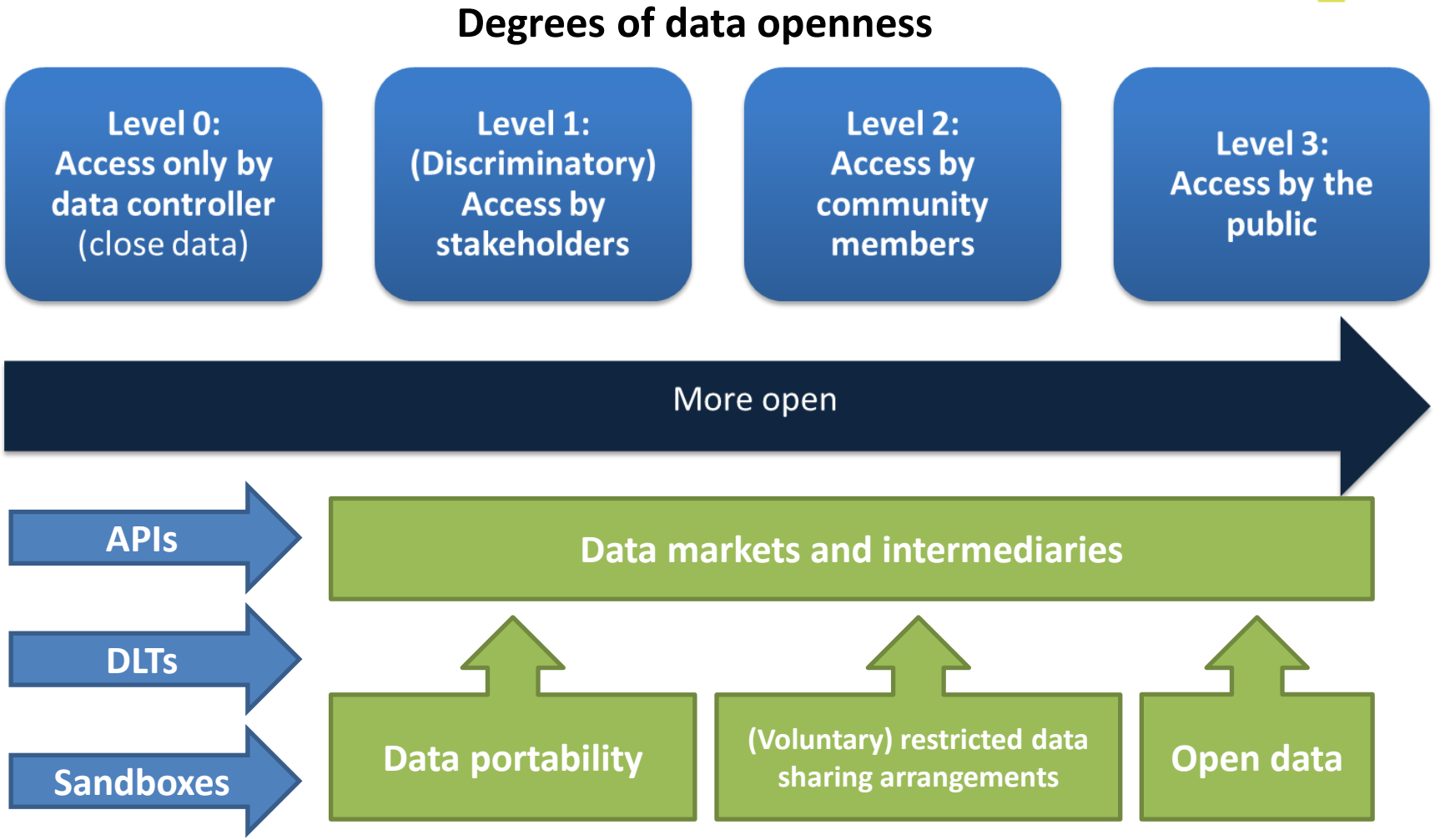
Cyentia Institute (2019), based on Advisen's Cyber Loss Data that tracks several different types of cyber events such as ransomware, privacy, denial of service, etc. They compile information from publicly-available sources such as breach disclosures, company filings, litigation details, Freedom of Information 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

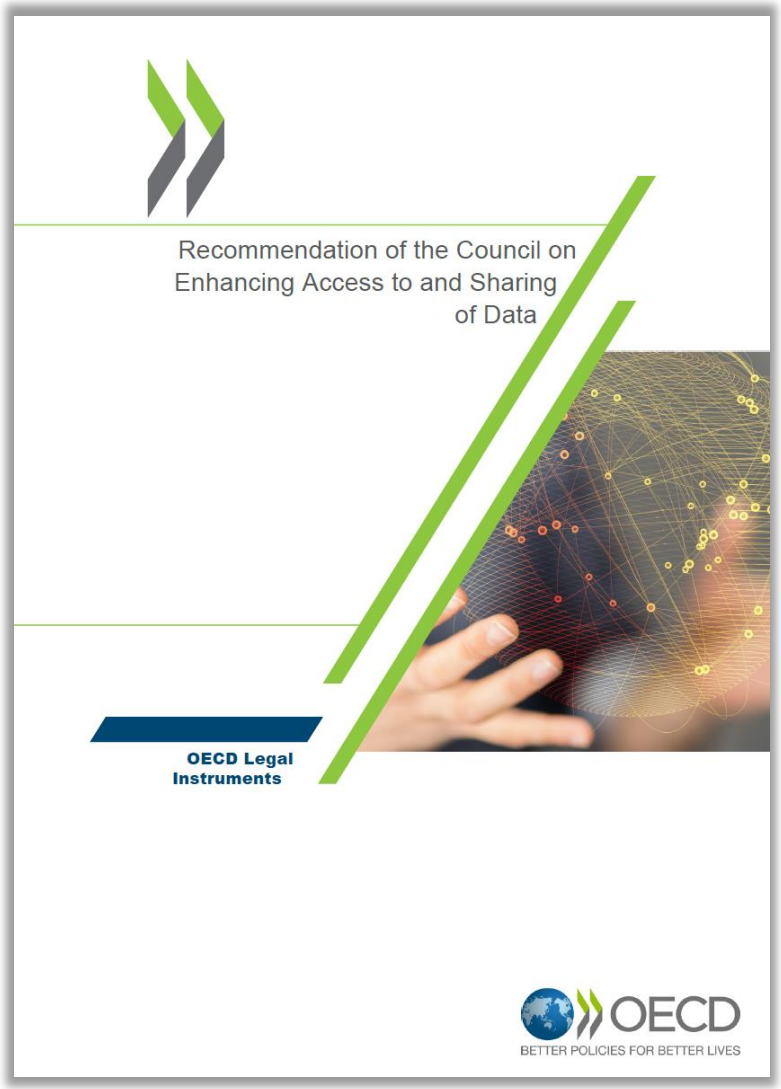


OECD (2015), "Drawing value from data as an infrastructure", in *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://doi.org/10.1787/9789264229358-8-en.

THE OECD COUNCIL RECOMMENDATION ON EASD

BETTER POLICIES FOR BETTER LIVES

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

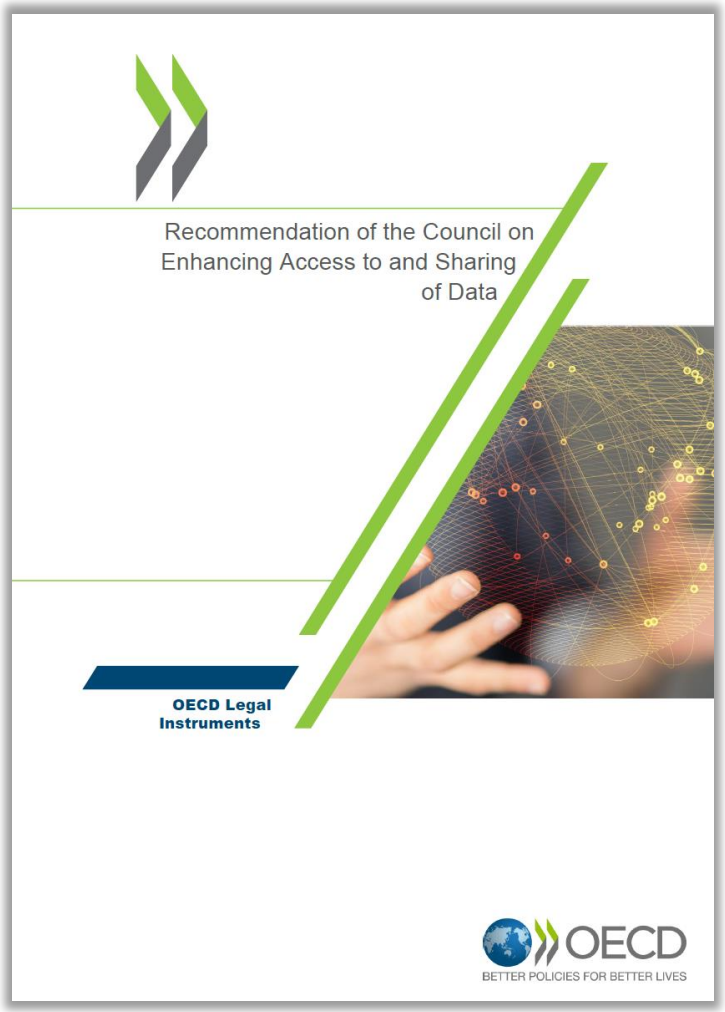
Digital economy

- 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 Capacity building for effective use of data

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, www.oecd.org/sti/ieconomy/protecting-children-online.htm, www.oecd.org/internet/ieconomy/enhanced-data-access.htm, and www.oecd.org/digital/ieconomy/digital-security/