

The Brussels Effect

SURF / SCIPR Privacy en Security conferentie
30 juni 2022, Groningen

Marlon Domingus,
FG, EUR

Erasmus University Rotterdam

Credits: Henriette Dietz, Privacy Council, EUR
with whom I collaborated to understand
the EU data governance reform



The Erasmus University logo, featuring the word 'Erasmus' in a stylized, cursive script.

Agenda

1. Context & Geopolitics
2. The EU Data Strategy
3. Future Developments



Source: https://twitter.com/vestager/status/1338869405329936385?s=20&t=5SRv0MlcePG4byj_iH7D2Q

Privacy in Context - Processings of Personal Data in a Classic Context and Today's Context and Implications for Accountability, Legislation, Ethics and Trust

Classic Context		Today's Context	
Processings within one organization	↔	Processings beyond organization in temporary or structural collaboration	EU GDPR fit for purpose?
Processings executed by users using software (regression / classification: supervised learning)	↔	Processings executed by algorithms (unsupervised learning / reinforcement learning)	EU GDPR fit for purpose? AI Legislation?
Processing on site, in one country	↔	Processing in the cloud, cross borders	'CJEU Schrems II ruling'
Processings done by own staff; known people, under contract	↔	Processings done in collaborations with trusted and new (not yet trusted) partners, collaborators and service providers	EU Digital Services Act
Processings done on datasets	↔	Processings done on datalakes	EU GDPR fit for purpose?

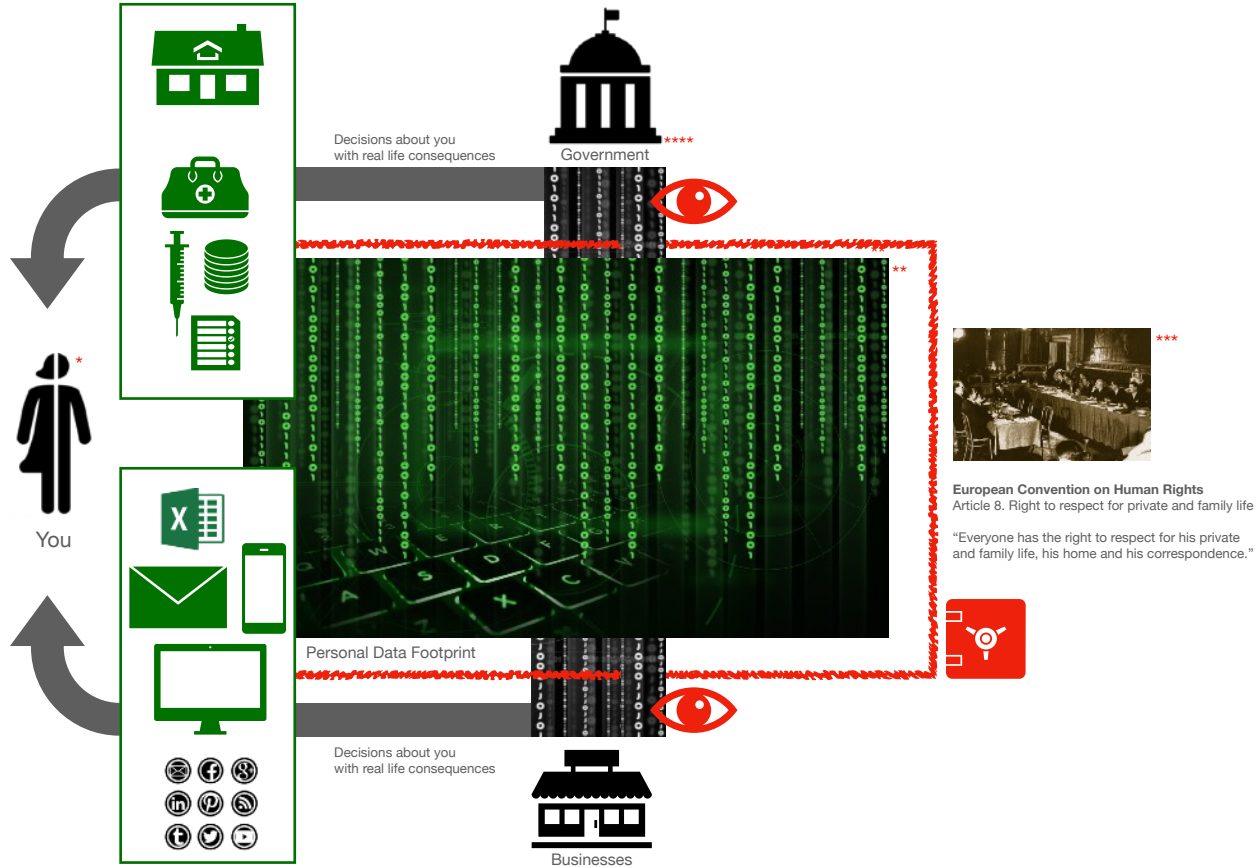


Inspired by work done by:

Helen Nissenbaum [Privacy in Context],
 Bojana Bellamy et al (CIPL) [CIPL Response to EU Consultation on AI White Paper]
 Marie-José Bonhuis [Privacy in Chain Communication Systems]



A View on Privacy



Marlon Domingus, Erasmus University Rotterdam
marlon.domingus@eur.nl September 2021

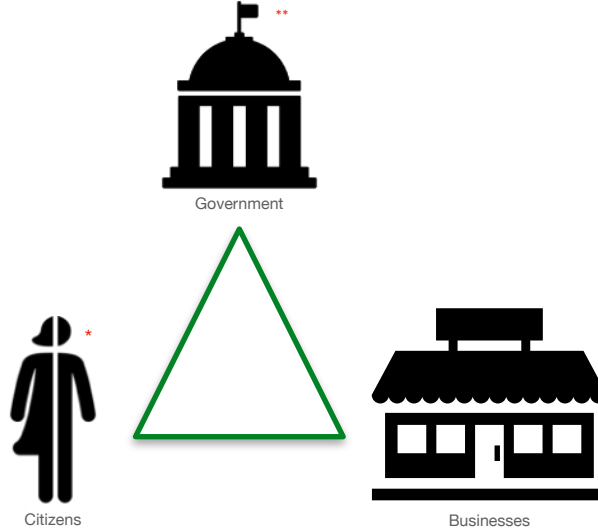
Credits: * Gender Neutral by Matt Brooks, the Noun Project. Source: <https://thenounproject.com/term/gender-neutral/14064/>

** Matrix image by PixxiTeufel from Pixabay

*** Signature of the European Convention on Human Rights. <https://www.echr.coe.int/Pages/home.aspx?p=basictexts>

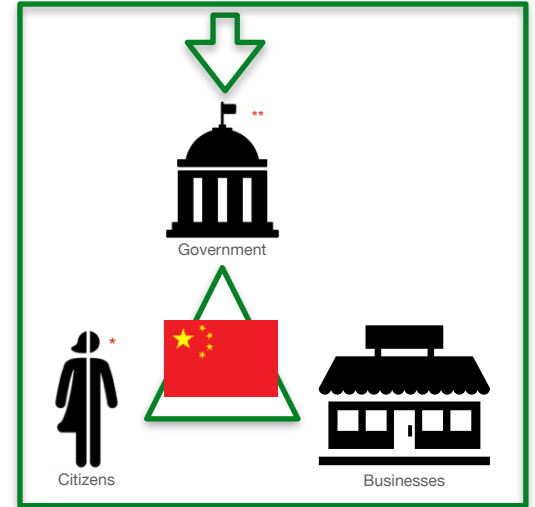
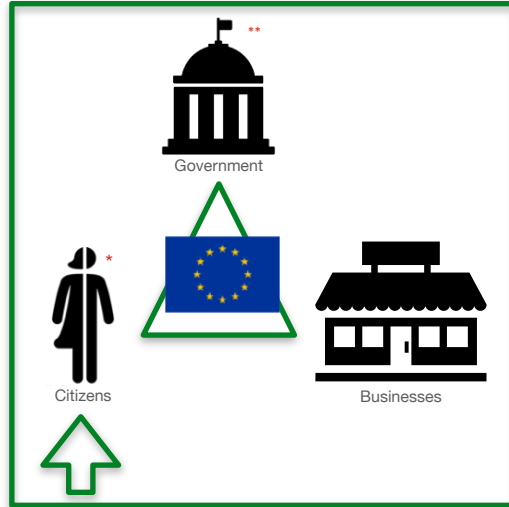
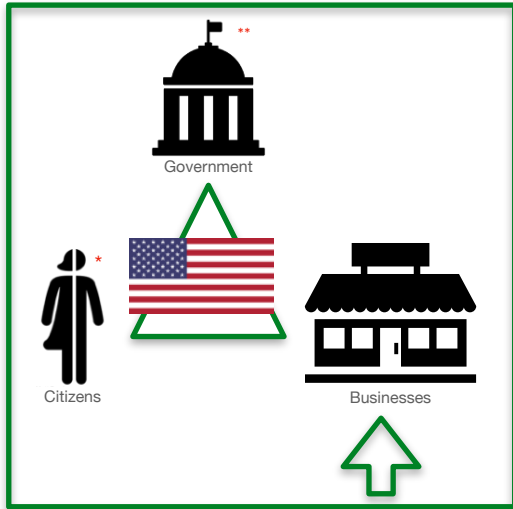
**** Government building by Adrien Coquet, the Noun Project. Source: <https://thenounproject.com/term/government-building/1101454/>

1. Context & Geopolitics: Qui Bono?



Erasmus

1. Context & Geopolitics: Qui Bono?

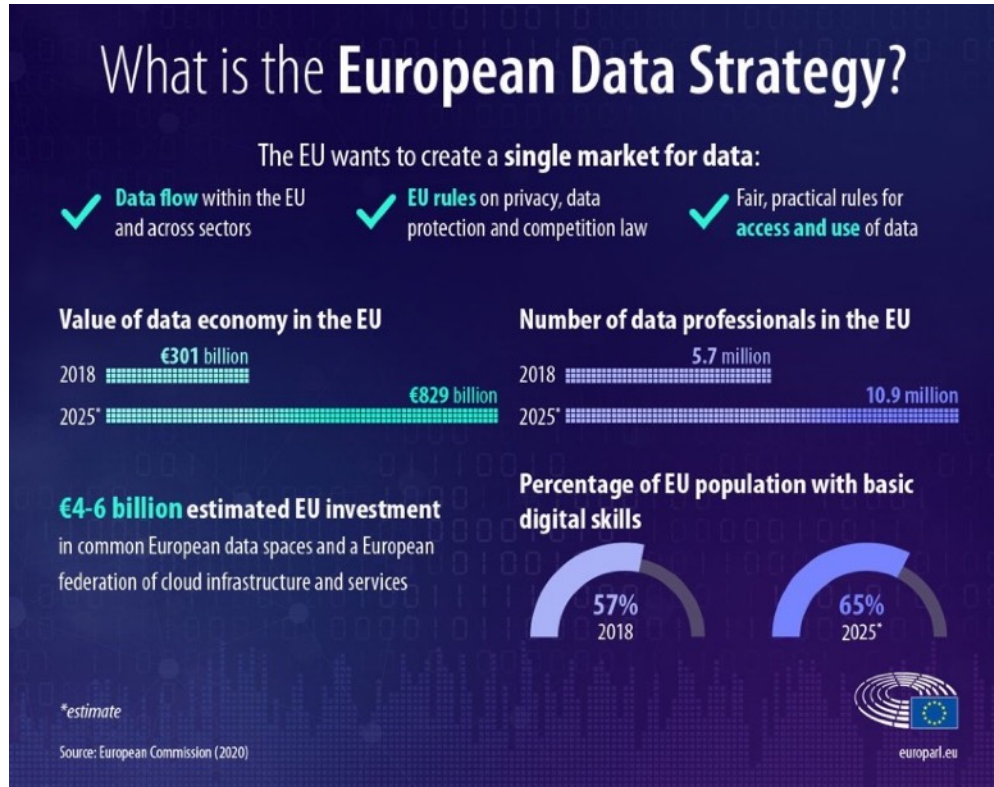


1. Context & Geopolitics



Erasmus

2. EU: The EU Data Strategy



Source: <https://pin.it/7fWnyyy>

2. EU: The EU Data Strategy

Het groeipotentieel van de data-economie

Gegevens vormen de basis van allerlei **nieuwe digitale producten en diensten**. De verbonden voorwerpen (het internet der dingen) die we gebruiken, **genereren alsmaar meer gegevens**.

Het mondiale datavolume blijft groeien

2018

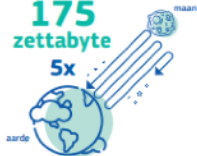
33 zettabyte



Als je dit opslaat op tablets met een capaciteit van 512 GB, krijg je een toren tot aan de maan.

2025

175 zettabyte



Genoeg voor vijf keer naar de maan en terug.

Een toename die gelijk is aan 1260 zulke tablets per seconde.

€5-11 biljoen



Mondiale waarde van het internet der dingen en gerelateerde diensten tegen 2030

€120 miljard



Jaarlijkse besparingen in de gezondheidssector van de EU

10-20%



Besparingen in de sectoren vervoer, gebouwen en industrie dankzij realtime-analyse van data

€270 miljard



Verwacht extra bbp van de 27 lidstaten tegen 2028 dankzij nieuwe gegevensregels

van 5% naar 10%



Bedrijven die investeren in datagestuurde innovatie kennen een 5% tot 10% snellere productiviteitsgroei



2. EU: The EU Data Strategy



In [the Commission's political agenda](#), [Commission President Ursula Von der Leyen](#) said that “digital technologies should enrich the lives of us all and respect European values”.

Home > Strategy > Priorities 2019-2024 > A Europe fit for the digital age


A Europe fit for the digital age

Empowering people with a new generation of technologies



Europe's Digital Decade

empowering businesses and people in a human-centred, sustainable and prosperous digital future




Shaping Europe's digital future

by making sure technology serves the people and adds value to their daily lives

Towards a digital Europe

The EU is investing in strategic digital capacities and the wide deployment of digital technologies. What does the digital transition mean for Europe's society and economy?

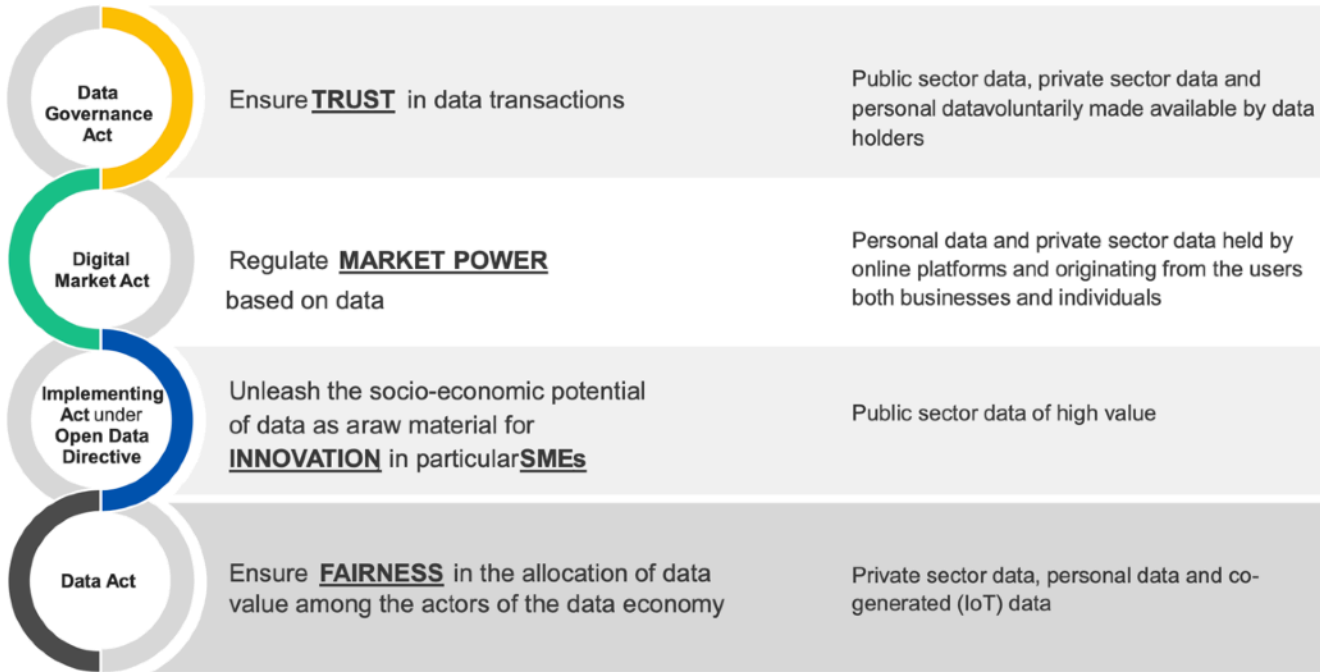
EU values at the heart of the digital transition



- transparency
- human rights
- security & safety
- data protection & privacy
- inclusivity
- fundamental freedoms
- democracy

2. EU: The EU Data Strategy

European Strategy for Data: 4 Key Instruments



Source: https://ec.europa.eu/eurostat/cros/system/files/03_data_governance_act.pdf

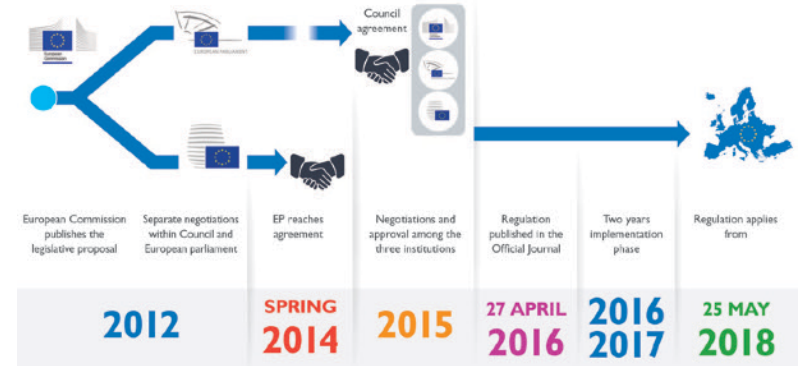
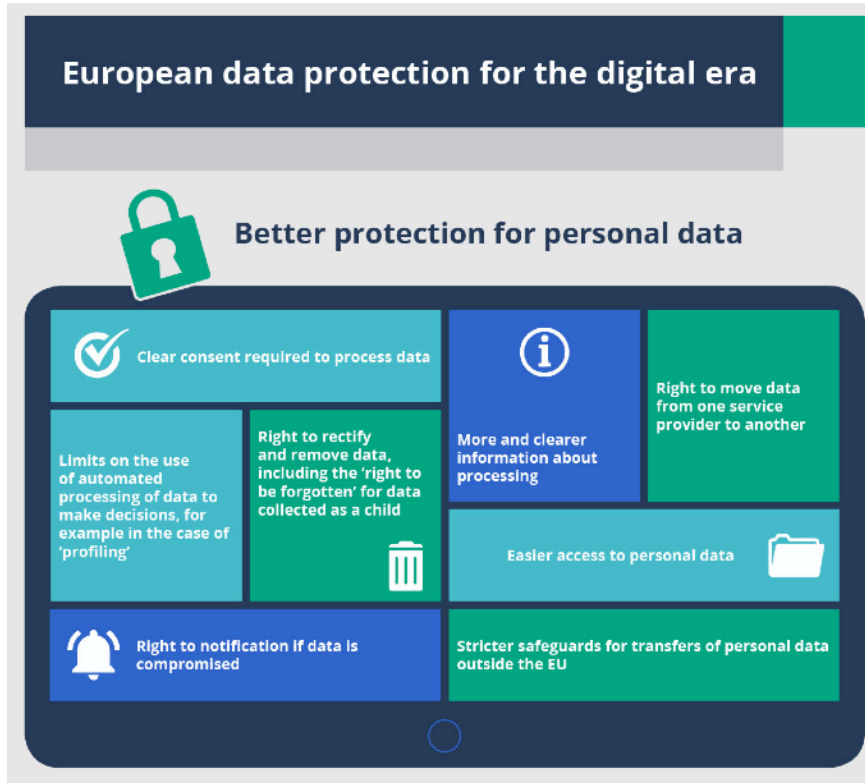
The EU Data Governance Reform



Marlon Domingus, Erasmus University Rotterdam
marlon.domingus@eur.nl March 2022

Name Act / Directive	Why	Status
<u>Digital Markets Act (DMA)</u> The Digital Services Act package	Aims to open digital market by establishing limits to current digital gatekeepers (aka big tech monopolies).	Published: 15 December 2020
<u>Digital Services Act (DSA)</u> The Digital Services Act package	Aims to re-shape the internet by altering the power imbalances between big dominant platforms and people using them. It is an update of the eCommerce Directive.	Published: 15 December 2020
<u>Data Governance Act (DGA)</u>	Aims at fostering the availability of data for use by increasing trust in data intermediaries and by strengthening data sharing mechanisms across the EU.	Published: 25 November 2020
<u>Data Act (DA)</u>	Aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation.	Published: 23 February 2022
<u>AI Act (AIA)</u>	Aims to ensure that AI systems placed on the EU market are safe and respect existing law on fundamental rights and EU values. To ensure legal certainty to facilitate investment and innovation in AI. To enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems. To facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.	Published: 21 April 2021
<u>Whistleblower Directive</u>	Aims to protect and encourage reporting of breaches of EU law. Whistle-blowers will be able to choose between internal and external reporting. Safeguards against reprisals from employers.	Adopted: 16 April 2019
<u>Database Directive</u>	Aims to legally protect databases in any form.	Adopted: 06 June 2019
<u>Open Data Directive</u>	Aims to govern re-use of public sector documents to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks.	Adopted: 20 June 2019
<u>ePrivacy Directive</u>	Aims to increase the protection of people's private life and open up new opportunities for business, by modernisation of the data protection framework for all electronic communications.	Published: 10 January 2017

2. EU: The EU Data Strategy: GDPR

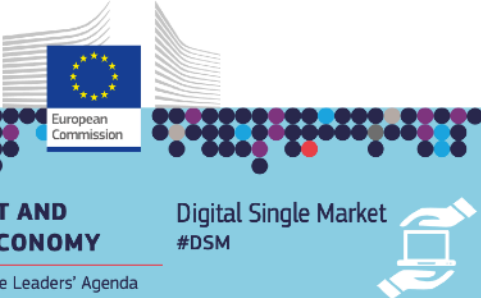


Erasmus

Source: www.consilium.europa.eu/en/infographics/data-protection-regulation-infographics/

Source: <https://www.dlapiper.com/no/uk/focus/eu-data-protection-regulation/background/>

2. ePrivacy Directive (aka the Cookie Directive)

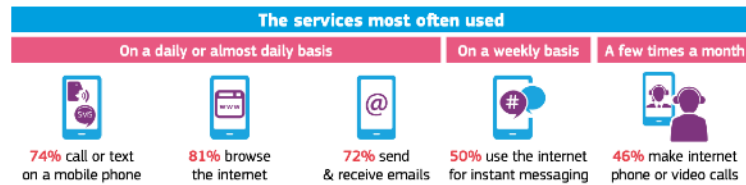


STRENGTHENING TRUST AND BOOSTING THE DATA ECONOMY

The Commission's Contribution to the Leaders' Agenda
#FutureOfEurope #EURoad2Sibiu
May 2018

Stronger privacy rules for electronic communications

The Commission has proposed on 10 January 2017 a Regulation on Privacy and Electronic Communications to update current rules to technical developments and to adapt them to the General Data Protection Regulation that will enter into application in May 2018. The objective is to reinforce trust and security in the Digital Single Market.



UPDATE OF CURRENT RULES





More and more Europeans use services such as Skype, WhatsApp, Facebook Messenger, Gmail, iMessage, or Viber to send messages or call. However, the current ePrivacy rules only cover traditional telecoms providers. To ensure that Europeans' electronic communications are confidential regardless of the technology used, the proposed rules will also apply to internet-based voice and internet-messaging services.

Will become the ePrivacy Regulation.





Relationship between General Data Protection Regulation & proposal for the ePrivacy Regulation

The General Data Protection Regulation protects personal data. The ePrivacy Regulation protects the confidentiality of electronic communications and the device.

General Data Protection Regulation

- Covers **all personal data** independently on the means of transmission. 
- Defines the right to personal data protection. 
- Introduces new rights for citizens and obligations for companies. 
- Starts to apply on 25 May 2018. 

Proposal for the ePrivacy Regulation

- Covers electronic communications and the **integrity of the information** on one's device, independently whether it is personal or non-personal data. 
- Right to the privacy and confidentiality of communications. 
- Ensures that mobile apps or internet services through which you communicate cannot intercept, record, listen into, or tap in your communications. 
- Proposed on 10 January 2017 and currently in the legislative process in the European Parliament and the Council. 

The proposal for the ePrivacy Regulation complements General Data Protection Regulation in the electronic communications sector.

When communications include personal data, the general rules of the General Data Protection Regulation apply, unless the ePrivacy Regulation lays down more specific rules.

2. ePrivacy Directive (aka the Cookie Directive)

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

(2012/C 326/02)

TITLE II FREEDOMS

Article 6

Right to liberty and security

Everyone has the right to liberty and security of person.

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Relationship between General Data Protection Regulation & proposal for the ePrivacy Regulation

The General Data Protection Regulation protects personal data. The ePrivacy Regulation protects the confidentiality of electronic communications and the device.

General Data Protection Regulation

1. Covers **all personal data** independently on the means of transmission.



2. Defines the right to personal data protection.



3. Introduces new rights for citizens and obligations for companies.



4. Starts to apply on 25 May 2018.



Proposal for the ePrivacy Regulation

1. Covers electronic communications and the **integrity of the information** on one's device, independently whether it is personal or non-personal data.



2. Right to the privacy and confidentiality of communications.



3. Ensures that mobile apps or internet services through which you communicate cannot intercept, record, listen into, or tap in your communications.



4. Proposed on 10 January 2017 and currently in the legislative process in the European Parliament and the Council.



The proposal for the ePrivacy Regulation complements General Data Protection Regulation in the electronic communications sector.

When communications include personal data, the general rules of the General Data Protection Regulation apply, unless the ePrivacy Regulation lays down more specific rules.

2. ePrivacy Directive (aka the Cookie Directive)

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

(2012/C 326/02)

TITLE II
FREEDOMS

Article 6

Right to liberty and security

Everyone has the right to liberty and security of person.

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8





Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.





Relationship between General Data Protection Regulation & proposal for the ePrivacy Regulation

The General Data Protection Regulation protects personal data. The ePrivacy Regulation protects the confidentiality of electronic communications and the device.

General Data Protection Regulation

1. Covers all personal data independently on the means of transmission. 
2. Defines the right to personal data protection. 
3. Introduces new rights for citizens and obligations for companies. 
4. Starts to apply on 25 May 2018. 

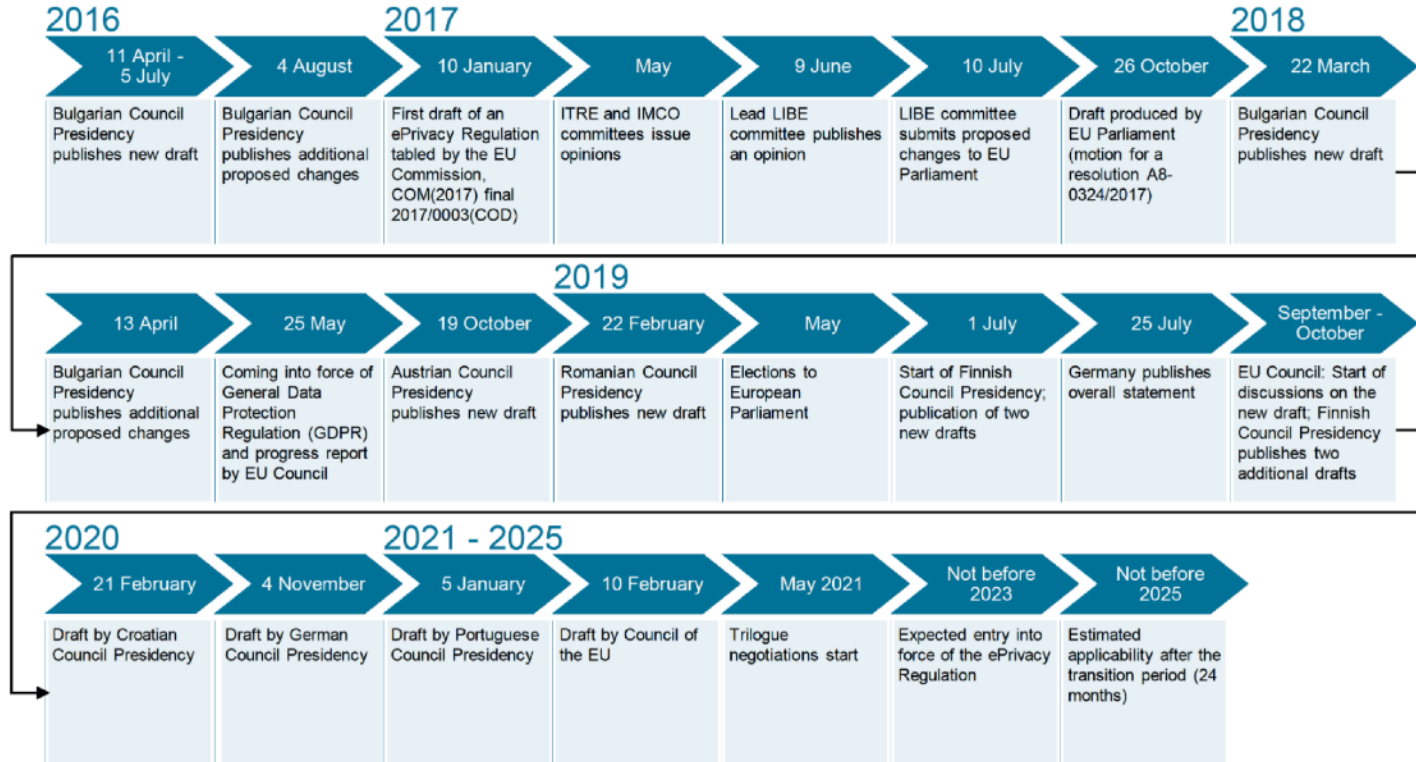
Proposal for the ePrivacy Regulation

1. Covers electronic communications and the integrity of the information on one's device, independently whether it is personal or non-personal data. 
2. Right to the privacy and confidentiality of communications. 
3. Ensures that mobile apps or internet services through which you communicate cannot intercept, record, listen into, or tap in your communications. 
4. Proposed on 10 January 2017 and currently in the legislative process in the European Parliament and the Council. 

The proposal for the ePrivacy Regulation complements General Data Protection Regulation in the electronic communications sector.

When communications include personal data, the general rules of the General Data Protection Regulation apply, unless the ePrivacy Regulation lays down more specific rules.

2. ePrivacy Regulation - Timeline



Ezafus

2. EU Digital Services Package (DSA & DMA)

EU Digital Services Package

Digital Services Act

Ensure a safe and proper functioning of the Digital Single Market

Digital Markets Act

Ensure fair, contestable and open markets for digital services

Scope

Intermediary Services

Online Platforms

Online Marketplaces 

Content Sharing 

Social Networks 

App Stores 

Very Large Online Platforms (VLOPs):
Specific rules for platforms reaching
10% of 450 million consumers in Europe

Cloud
Services 

Web
Hosting 

Core Platform Services

- Online intermediation
- Online search engines
- Social networks
- Video-sharing platforms
- Messaging services
- Operating systems
- Cloud computing

Gatekeeper Criteria

- Strong economic position: significant impact on internal market and active in multiple EU countries
- Important gateway: strong intermediation position
- Durable position and impact in the market

Other Market Features

- Entry barriers derived from network effects and data driven advantages
- Scale and scope effects the provider benefits from, including with regard to data
- Business user or end user lock-in effects



2. EU Digital Services Package (DSA & DMA)

DMA Do's and Don'ts

Examples of Do's:

- ✓ Must allow the installation & use of third-party software application stores that are interoperable with gatekeeper's core platform services.
- ✓ Allowing end users to continue accessing or using the relevant service through relevant eco-systems.
- ✓ Cannot treat own services more favourably in ranking services (e.g. in search algorithms), must provide such ranking services on a non-discriminatory basis.

Examples of Don'ts:

- ✗ Combining personal data from their core platform services with data from other sources (including other services offered by gatekeepers)
- ✗ Restricting business users from contracting with end users outside of the gatekeepers' eco-systems
- ✗ Requiring business users to use, offer or interoperate with any identification service of the gatekeeper in the context of providing its services via relevant gatekeeper's core platform services.

DSA

Hot Topics

DMA

Content:
Illegal vs
Harmful

Scope

Know Your
Business
Customer

Scope
Designation of
gatekeepers

List of
Do's & Don'ts

Market
investigation &
interim
measures

Notice & Action
Good Samaritan &
Trusted Flaggers

Digital
advertising
targeting

Supervision,
cross-border
cooperation &
fines

Enforcement
and monitoring
powers

Supervisory
framework

Fines, penalties,
behavioural
& structural
remedies

2. EU Digital Services Package (DSA & DMA)

Estimated Timeline



|=|
FLEISHMANHILLARD



2. Digital Markets Act (DMA)

Digital Markets Act

What is the Digital Markets Act (DMA)?

It is a new set of EU rules that will ensure **fair competition** on digital platforms.

ACT

← 1 dot = 1 SME online platform

Today, over **10 000** high-growth SME online platforms operate in the EU's digital economy.

Gatekeepers will not be allowed to:

- over-promote their own products
- limit payment possibilities to their own payment method
- re-use personal data collected during one service for the purposes of another service
- impose unfair conditions on business-users
- pre-install certain software applications
- restrict business users of platforms
- use certain bundling practices
 - selling different items as a package

Companies that do not comply with the new obligations may risk fines of up to 10% of their worldwide turnover.

2. Digital Services Act (DSA)

Digital Services Act


What is the Digital Services Act (DSA)?

The DSA is an essential part of the EU's digital agenda that aims to create a **safe digital space** for citizens and businesses.

Today, e-commerce is an unstoppable trend. 2021 is a major milestone as the number of e-commerce users will **probably exceed 500 million**.



E-commerce per EU country ←

EUROPEAN UNION (2020)		
447.7 million population	73% e-shoppers	757 billion online sales (€)



The DSA's objectives are to:

- create a safer online environment
- define clear responsibilities for platforms such as marketplaces and social media
- deal with current digital challenges, which include:
 - illegal products, hate speech and disinformation
 - transparent data reporting and oversight



2. Data Governance Act (DGA)



European Commission

EUROPEAN DATA GOVERNANCE

A NEW APPROACH FOR THE DIGITAL DECADE

November 2020

Setting up a new European way of data governance will facilitate data sharing across sectors and Member States. It will create wealth for society, and provide control to citizens and trust to companies.

The economic value of data sharing

- ◆ Data access and reuse can generate **social and economic benefits of 1% to 2.5%** of GDP¹.
- ◆ The new measures could **increase the annual economic value** of data sharing by up to €7-11 billion by 2028².
- ◆ In addition, the new rules will have a **wider impact on the EU economy and society** as a whole.

€ 1.3 trillion
in increased productivity in **manufacturing** through **Internet-of-Things data** by 2027³

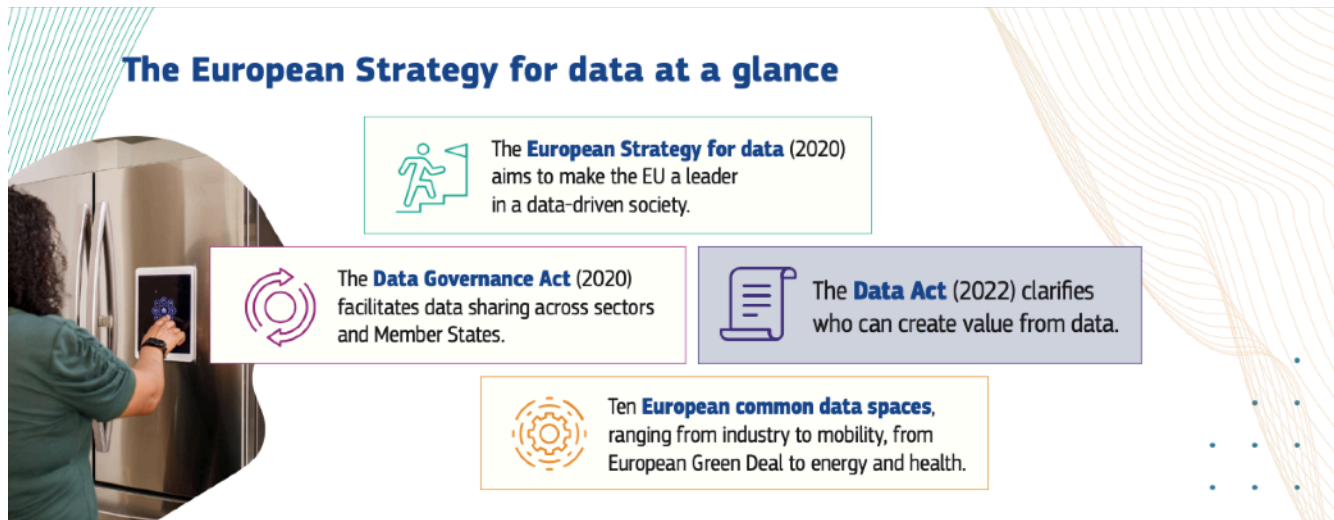
€ 120 billion
of savings per year in the **EU health sector**⁴

The EU will boost the development of **trustworthy data-sharing systems**:

- ◆ Empower **Europeans** to decide what happens to their data, and what data they would like to share with whom.
- ◆ Facilitate **data altruism** to make it easier and safer for companies and individuals to voluntarily make their data available for the benefit of society.
- ◆ Enhance the **reuse** of public sector data that cannot be made available as open data.
- ◆ Create **new EU rules on neutrality** to allow novel data intermediaries to function as trustworthy organisers of data sharing.
- ◆ Set up a **European Data Innovation Board** to steer data governance and prioritise standards.



2. Data Act (DA) - *Complements DGA*



The Data Act addresses the legal, economic and technical issues that lead to data being under-used. The new rules will make more data available for reuse and are expected to create €270 billion of additional GDP by 2028.

2. Data Act (DA)



European
Commission

DATA ACT

THE PATH TO
THE DIGITAL DECADE

#DigitalEU 23 February 2022

The Data Act will make **more data available** for use. It will set up rules on who can use and access what data for which purposes across all economic sectors in the EU.

The growth potential of the data economy

Data is the basis for many **new digital products and services**. The use of connected objects (Internet of Things) increasingly **generates data**.

Global data volume will grow

2018

33 zettabytes



Stored on 512 GB tablets, it would form a tower that reaches the moon.

2025

175 zettabytes



Enough to make the journey to the moon and back five times.

A growth equivalent to 1260 tablets per second.

€5-11 trillion



Internet of things value and services by 2030 globally

€ 120 billion



Savings in the EU health sector per year

10-20%



Savings in the transport, buildings and industry sectors with real-time analytics of data

€270 billion



Expected EU-27 additional GDP by 2028 thanks to new Data rules

5% to 10%



Companies investing in **data-driven innovation** exhibit faster productivity growth by 5% to 10%



2. AI Act (AIA)

Preparation of the proposal

Following the [White Paper on Artificial Intelligence](#)⁶ adopted in February 2020, the Commission launched a broad [public consultation](#) in 2020 and published an [Impact Assessment of the regulation on artificial intelligence](#), a supporting [study](#) and a [draft proposal](#), which received [feedback](#) from a variety of stakeholders.⁷ In its impact assessment, the Commission [identifies six main problems](#) raised by the development and use of AI systems, due to their specific characteristics.⁸

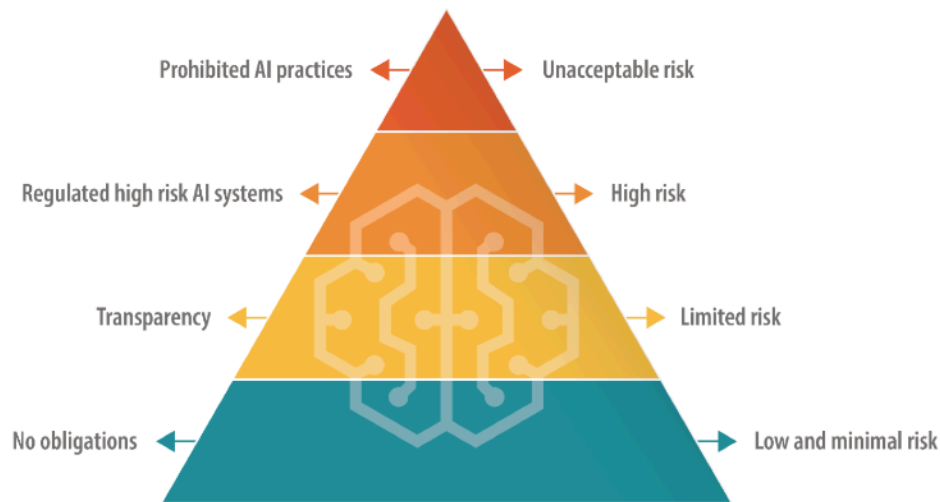
- The use of AI poses increased risks to citizens' safety and security.
- Use of AI poses increased risks of violations of citizens' fundamental rights and Union values.
- Authorities do not have the powers, procedural frameworks and resources to ensure and monitor AI development and use complies with applicable rules.
- Legal uncertainty and complexity on how existing rules apply to AI systems dissuade businesses from developing and using AI systems.
- Mistrust in AI would impede AI development in Europe and reduce the global competitiveness of the EU economy.
- Fragmented measures create obstacles for the cross-border AI single market and threaten the Union's digital sovereignty.

The logo for Erasmus, featuring a stylized, handwritten-style script of the word "Erasmus" in a dark blue or black color.

2. AI Act (AIA)

Pyramid of risks

The use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour), can adversely affect a number of fundamental rights and users' safety. To address those concerns, the draft AI act follows a **risk-based approach** whereby legal intervention is tailored to concrete level of risk. To that end, the draft AI act distinguishes between AI systems posing (i) **unacceptable risk**, (ii) **high risk**, (iii) **limited risk**, and (iv) **low or minimal risk**. Under this approach, AI applications would be regulated only as strictly necessary to address specific levels of risk.²⁰

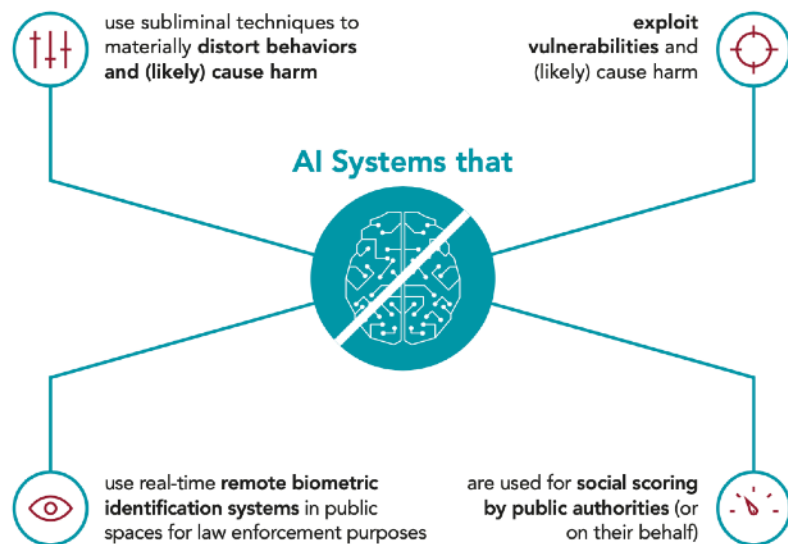


Erasmus

2. AI Act (AIA)

PROHIBITED USES

The Regulation identifies a series of AI practices that are prohibited because they go against the EU values or because they violate EU individuals' fundamental rights.

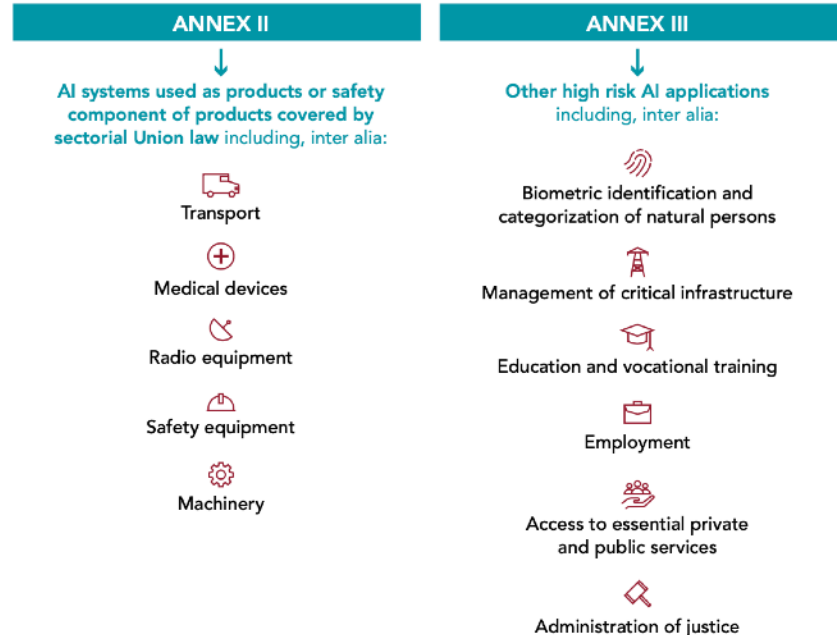


Erasmus

2. AI Act (AIA)

HIGH-RISK AI SYSTEMS

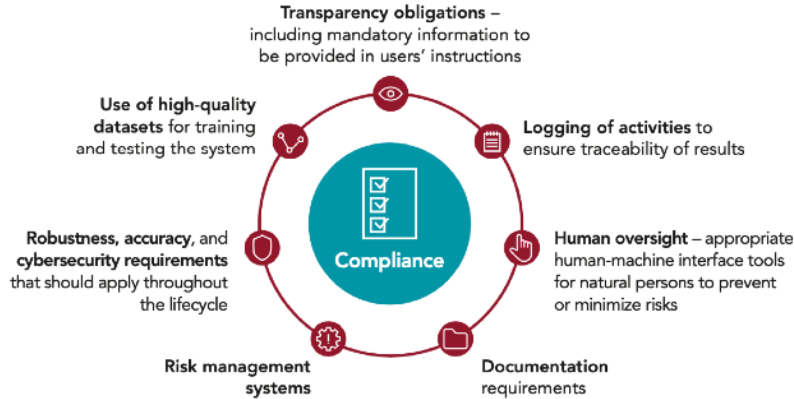
The proposal primarily focuses on high-risk AI applications and impose **stringent requirements** on **'providers'** and **'users'** of AI applications, as well as across the supply chain. In-scope uses are listed in 2 annexes.



2. AI Act (AIA)

EX-ANTE REQUIREMENTS VETTED BY A CONFORMITY ASSESSMENT

Before the placement of AI systems on the market or their putting into service, high-risk AI systems should undergo a **conformity assessment** to ensure they are in line with the requirements of the Regulation.



2. Whistleblower Directive



Directorate-General for
Justice and Consumers



Recent scandals, from LuxLeaks to Panama and Paradise Papers or Cambridge Analytica, were brought to the attention of the authorities and the media by whistleblowers.

Who is a “whistleblower”?

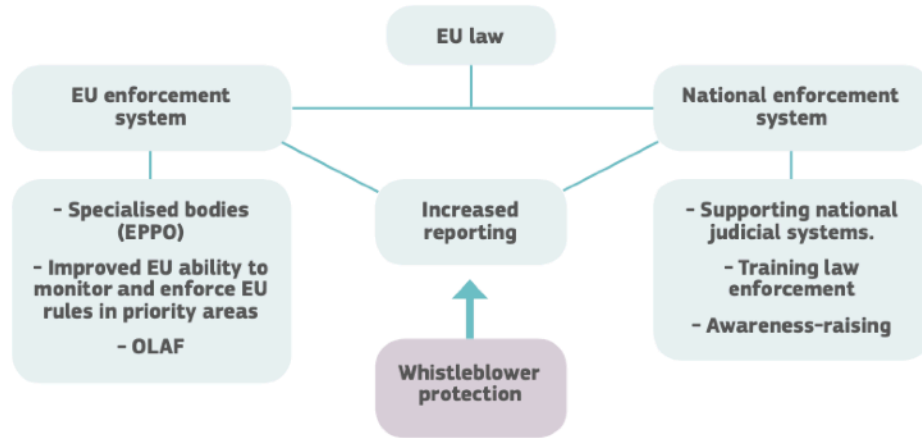
Whistleblowers are people speaking up when they encounter, in the context of their work, wrongdoing that can harm the public interest, for instance by damaging the environment, public health and consumer safety and EU public finances.

Source: https://ec.europa.eu/info/sites/default/files/placeholder_11.pdf

2. Whistleblower Directive

What role do they play in enforcing EU law?

Whistleblowers' reports can lead to effective detection, investigation and prosecution of violations of EU law that would otherwise remain hidden, causing serious harm to the well-being of society and, generally, to the public interest.



2. Whistleblower Directive

The main problems

Protection of whistleblowers is fragmented across the EU and uneven across policy areas

Currently, only ten EU countries (France, Hungary, Ireland, Italy, Lithuania, Malta, Netherlands, Slovakia, Sweden and United Kingdom) have a comprehensive law protecting whistleblowers. In the remaining EU countries, the protection granted is partial: it covers only public servants or only specific sectors (e.g. financial services) or only specific types of wrongdoings (e.g. corruption). Recent scandals uncovered by whistleblowers illustrate how insufficient protection in one country not only negatively impacts the functioning of EU policies there, but can also spill over into other countries and into the EU as a whole.

At EU level, there is only a very limited number of sectors where measures have been put in place to protect whistleblowers (mostly only in the areas of financial services).

What will the new proposal bring?

The proposal will guarantee a high level of protection for whistleblowers who report breaches of EU law by setting new, EU-wide standards. The new law will establish safe channels for reporting both within an organisation and to public authorities. It will also protect whistleblowers against dismissal, demotion and other forms of retaliation and require national authorities to inform citizens and provide training for public authorities on how to deal with whistleblowers.

Awareness about the protection of whistleblowers



49%

of citizens

did not know where to report corruption



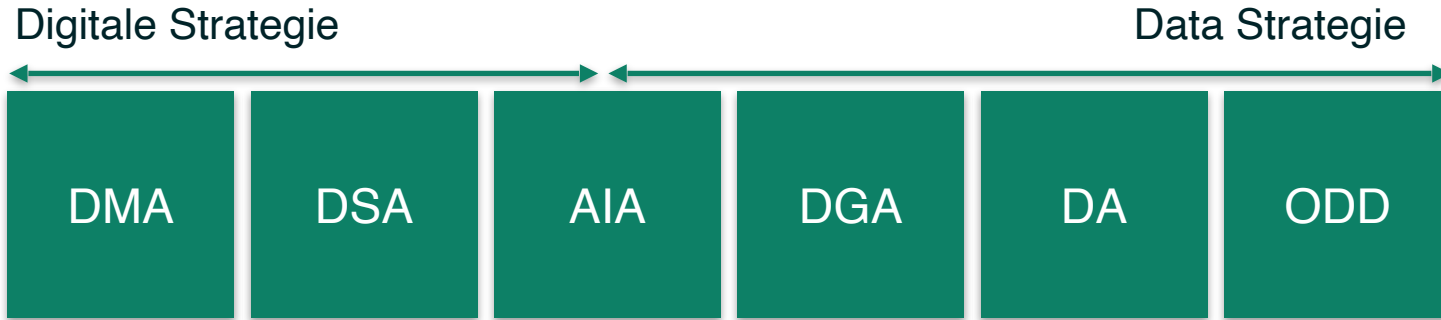
15%

of citizens

know about existing rules on whistleblower protection



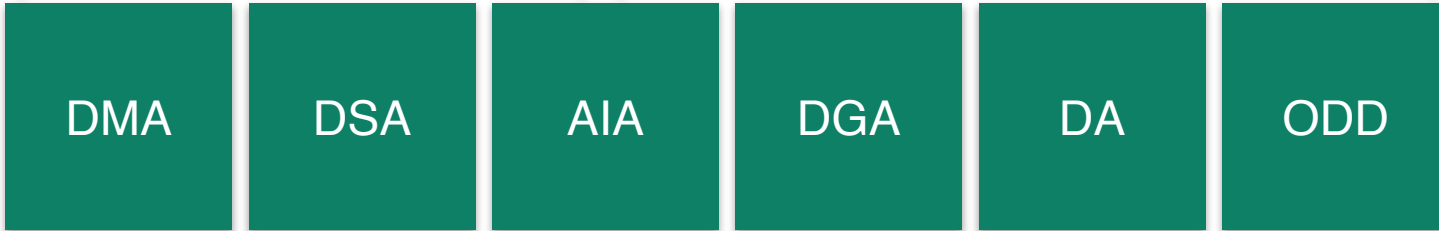
2. EU: The EU Data Strategy: Impact Hoger Onderwijs NL



2. EU: The EU Data Strategy: Impact Hoger Onderwijs NL

Digitale Strategie

Data Strategie



HO
2022

Formuleren compliancy eisen DMA/DSA/AIA
tbv toetsingskader inkoop / aanbestedingen
mbt **diensten van derden** en **diensten van de
EUR**.

Randvoorwaarden: Procedures / Support

Instellingen / SURF / UNL / SLM Rijk / ...

Voorsorteren op EUR compliancy DGA/DA/ODD, om te kwalificeren
als geregistreerd **Data-Intermediair** (DGA) en **Datadeeldienst**
(ODD) tbv hergebruik van data voor EUR onderzoek.

Randvoorwaarden: Beleid / Procedures / IV&IT / Beheer / Support

Instellingen / SURF / UNL / SLM Rijk / ...

3. Future Developments

New Legal Concepts:

- “Very Large Online Platforms” (VLOPs) - (DSA)
- “Notice and take action mechanisme” - (DSA)
- “Trusted Flaggers” - (DSA)
- “Gatekeepers” - (DMA)
- “Unfair Conditions” - (DMA)
- “Data altruism” - (DGA)
- “Data intermediation service” / “Services of data cooperatives” - (DGA)
- “Rulebook* for recognized data altruism organizations”
(technical and security requirements, communication roadmaps, interoperability standards) - (DGA)
- “Data Holder” - (DGA)
- “Data User” - (DGA)
- “Prohibited AI practices” -> unacceptable risk - (AIA)
- “Regulated high risk AI systems” -> high risk - (AIA)
- “Regulatory Sandboxes” - (AIA)
- “Digital Sovereignty” - (AIA)

The logo for Erasmus, featuring a stylized, handwritten-style script of the word "Erasmus" in black.

* Source: <https://data.consilium.europa.eu/doc/document/ST-14606-2021-INIT/en/pdf>

3. Future Developments

New (Supervisory) Bodies:

- European Data Innovation Board (DGA)
- Digital Services Coordinator (DSA)
- European Supervisor (DMA)
- ...

Risks:

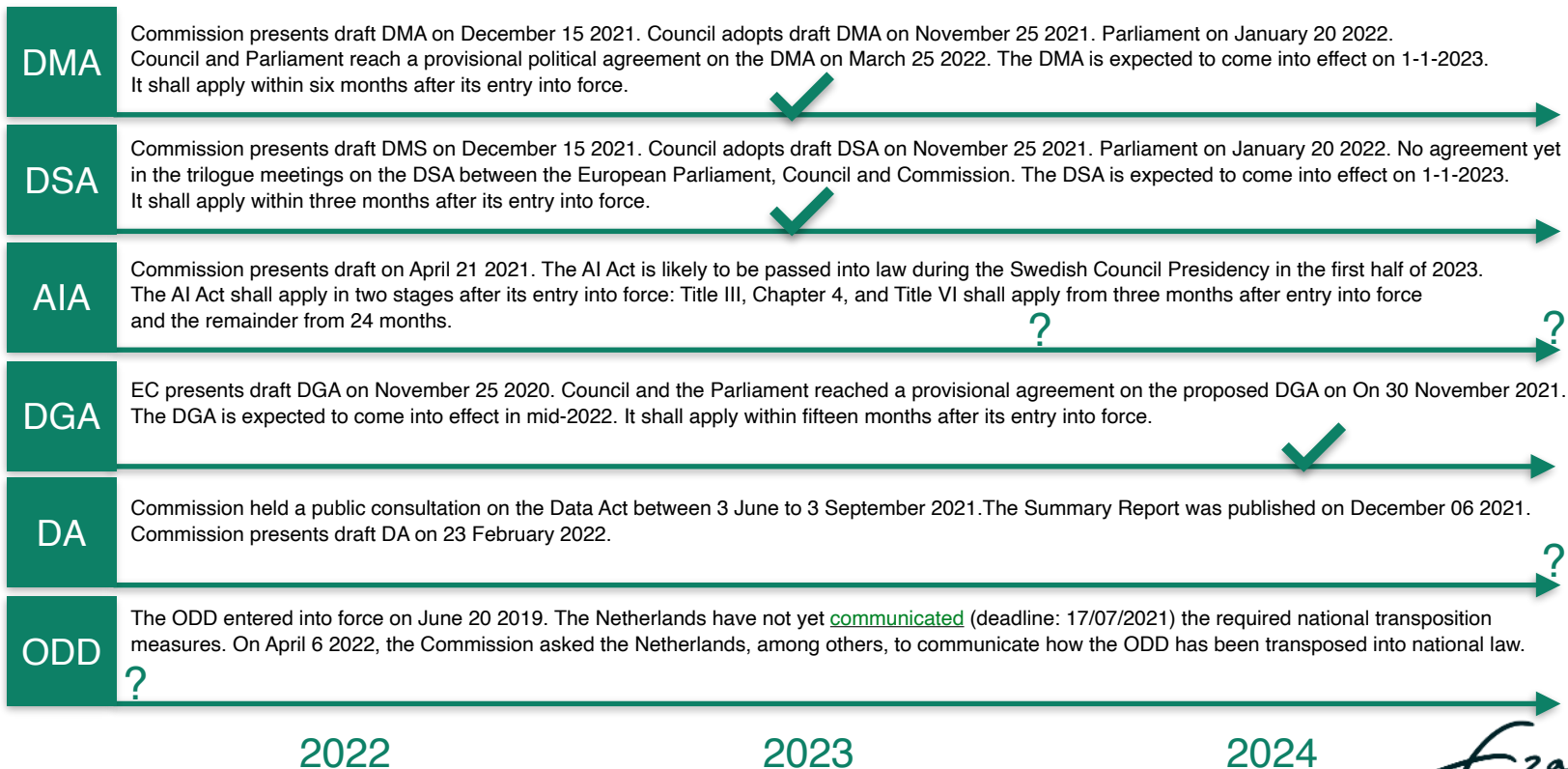
- No formal practical guidance for implementation
- Legal framework / hierarchy / interpretation of concepts

Opportunities:

- Human-centered way of thinking and working

The Erasmus logo is a stylized, handwritten-style signature of the word "Erasmus" in black ink, located in the bottom right corner of the slide.

3. Timeline



Erasmus





drs. Marlon Domingus, CIPP/e, CIPM

Data Protection Officer

Erasmus University Rotterdam

dpo@eur.nl

Erasmus