

GDPR TRAINING



Overview

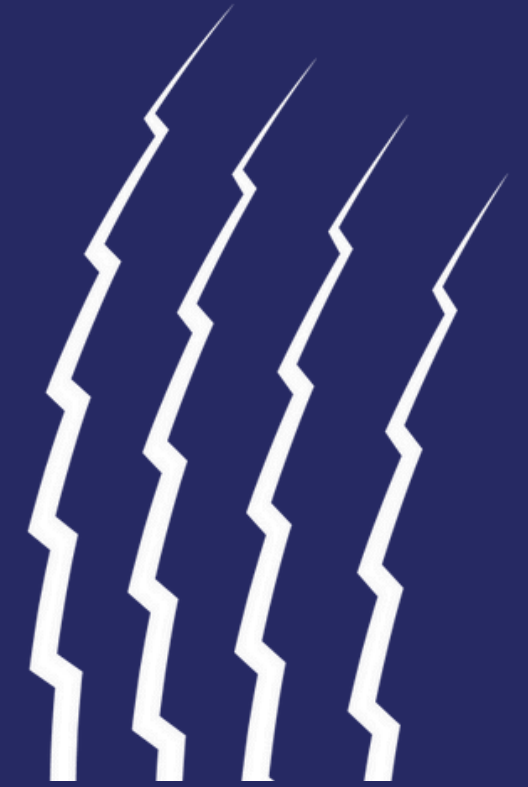
- Origins of GDPR
- Personal Data - Definition
- Principles of GDPR
 - Data Subject Rights
- Enforcement
- Compliance
 - Obligations of C&S C'ttee Members
 - Data Breaches
 - Data Subject Access Requests



Human Rights



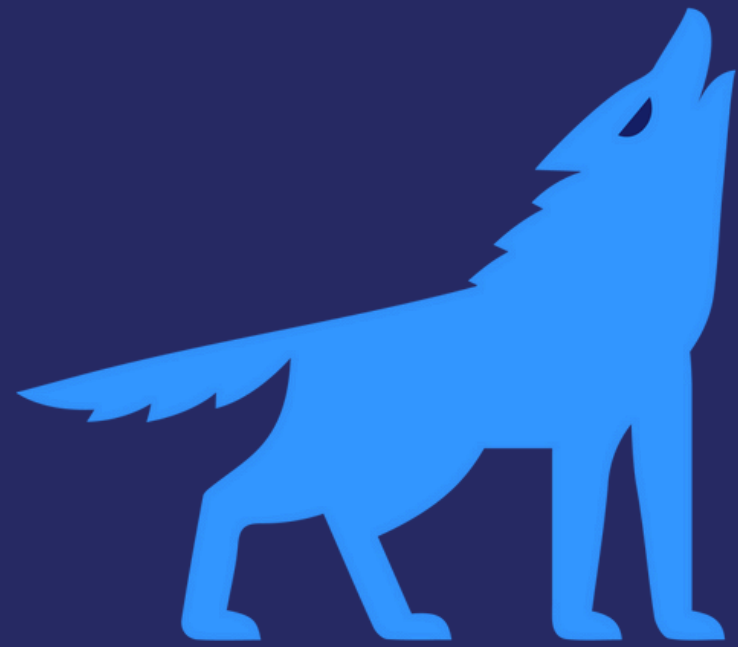
Origins - European Convention of Human Rights Article 8



European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society".

Article 8 – Right to respect for private and family life

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.



Context - Historical development of Privacy Legislation

- 1948 Universal Declaration of Human Rights
- 1953 European Convention on Human Rights
- 1980 Org.Economic Cooperation & Development (OECD) Guidelines
- 1995 Data Privacy Directive 95/46/EU
- 2000 Charter of Fundamental Rights
- 2002 e-Privacy Directive
- 2016 General Data Protection Regulation

Personal Data



In accordance with Article 4(1) of the General Data Protection Regulation (GDPR), personal data is defined as any information relating to an identified or identifiable natural person ('data subject')

- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.



Additional information
not used for identification
(info)

Personal
data

Identifier
(id)

Person

Health

Relatives

Education

Believes

Property



DNA

Personal
id

Full name

User ID

Browser
Cookies

Geo-location

Other
identifier...

Financial
transactions

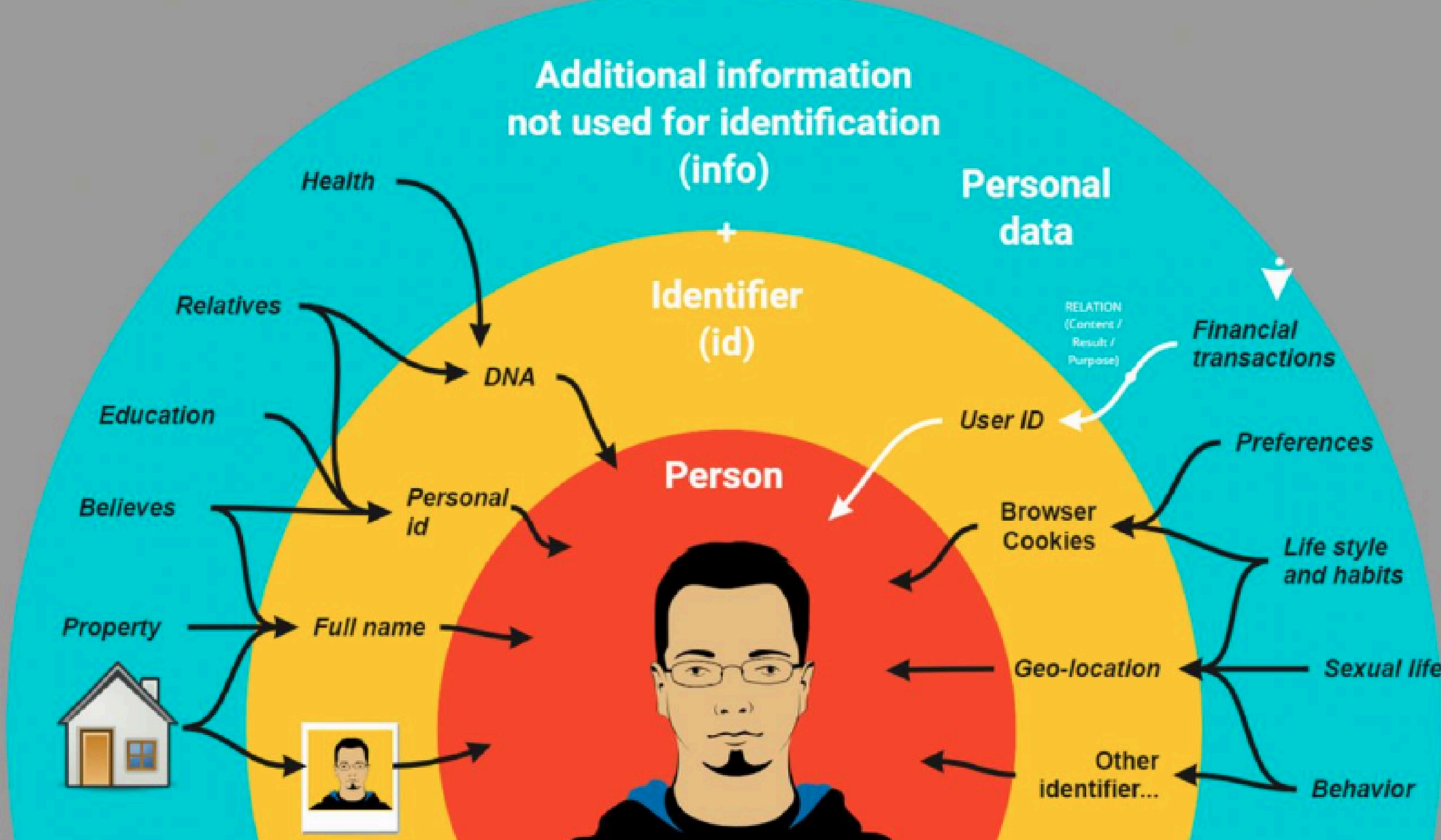
Preferences

Life style
and habits

Sexual life

Behavior

RELATION
(Content /
Result /
Purpose)



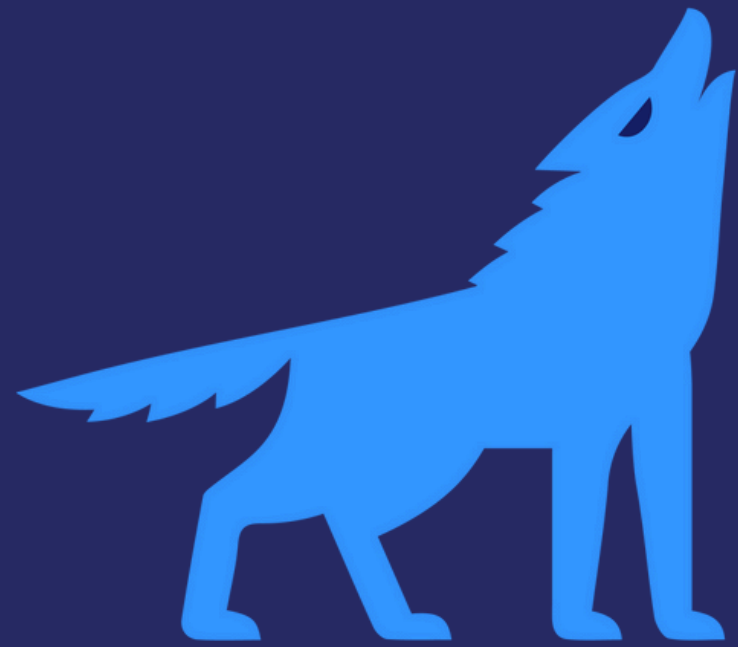
Special (or 'Sensitive') Personal Data

- Racial or Ethnic Origin
- Political opinion
- Religious or Philosophical Beliefs
- Trades Union Membership
- Biometric and Genetic Data
- Criminal Convictions
- Health Data
- Sex Life, or Sex Orientation



Principles





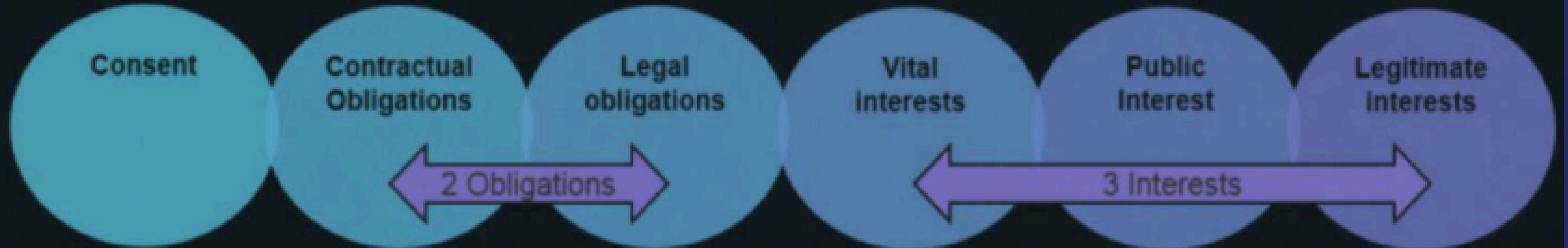
Fundamental Principles

- Article 5 GDPR

Personal Data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in line with subject's rights
- Kept secure
- Not transferred to countries without adequate protection

Principle 1 - Lawfulness of processing



Consent

Data subject gives consent for one or more specific purposes

Contractual

Processing is necessary to meet contractual obligations entered into by the data subject.

Legal

Processing is necessary to comply with legal obligations of the controller.

Vital Interests

Processing is necessary to protect the vital interests of the data subject

Public Interest

Processing is necessary for tasks in the public interest or exercise of authority vested in the controller.

Legitimate Interests

Processing is for the purposes of legitimate interests pursued by the controller.

Note these 2 lawful bases are not absolute and subjects may have a right to object

Rights of Data Subjects

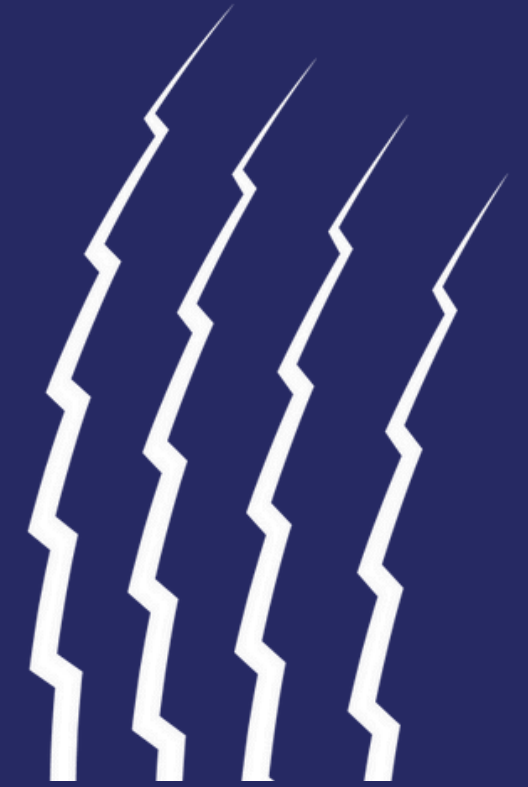


- Right to be informed
- Right of access
- Right to rectification
- Right to restrict processing
- Right to data portability
- Right to object to processing or storage
- Rights in relation to automated decision making
- and profiling

Enforcement



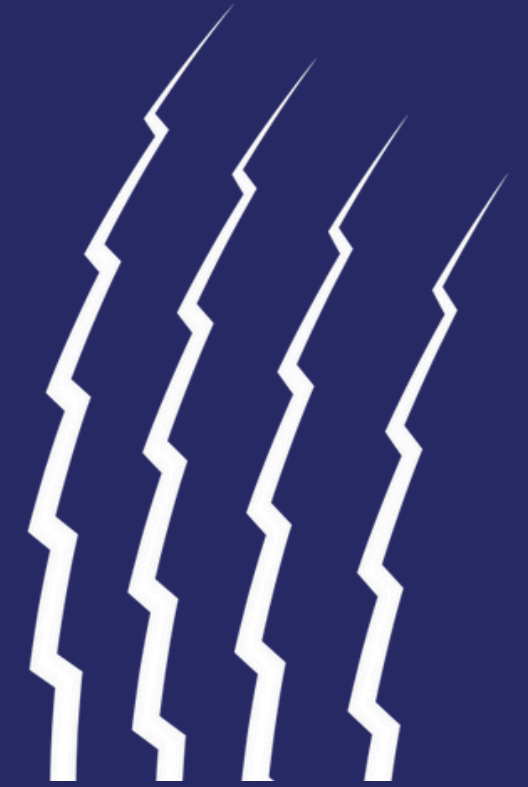
Office of the Data Commissioner - Growth



1. Budget

- 2016: The DPC's budget was relatively modest at around €3.65 million.
- 2018: The introduction of the GDPR led to a major increase in responsibilities for the DPC, resulting in the budget increasing to €11.7 million.
- 2019: The budget grew to around €15.2 million.
- 2020: The DPC's funding was further increased to €16.9 million, reflecting the growing demands on the office.
- 2021: The budget allocation reached approximately €19.1 million.
- 2022: Funding continued to rise to around €23.2 million.
- 2023: The budget climbed to approximately €26.2 million.

Office of the Data Commissioner - Growth



2. Personnel

- 2016: The office had about 30 employees.
- 2018: By the time GDPR came into effect, staff numbers had more than doubled, with the DPC employing 110 people.
- 2019: The number of staff increased to about 140.
- 2020: The DPC employed around 145 people, as the office struggled to keep up with demand and increased investigations.
- 2021: Staffing levels rose to approximately 190 employees.
- 2022: The workforce expanded to about 200 employees.
- 2023: The office continued expanding, with around 210–220 staff



Irish data watchdog to probe Facebook for listening to Messenger audio conversations



DPC Approach



- Own Volition Inquiries
- Complaints
- Inspection / Audit
- Legal Action / Stop Processing
Orders / Fines

Supervisory Authority Fines Issued 2018 - 2023

Enforcement Tracker



GDPR Enforcement Tracker

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and penalties](#). Please note that we do not list any fines imposed under national / non-European laws (with the exception of fines under the UK GDPR), under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.





























New features: "ETid" and "Direct URL"

We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 25 entries

Search:


ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<small>Filter Column</small>	<small>Filter Column</small>		<small>Filter Column</small>	<small>Filter Column</small>		<small>Filter Column</small>	
ETid-1844	IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing	link link
ETid-1373	IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles	link link
ETid-1543	IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles	link
ETid-2032	IRELAND	2023-09-01	345,000,000	TikTok Limited	Art. 5 (1) c), 5 (1) f) GDPR, Art. 12 (1) GDPR, Art. 13 (1) e) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR	Non-compliance with general data processing principles	link
ETid-1502	IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link link
ETid-820	IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations	link link
ETid-2461	IRELAND	2024-09-27	91,000,000	Meta Platforms Ireland Limited	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR, Art. 33 (1), (5) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-979	FRANCE	2021-12-31	60,000,000	Google Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing	link link
ETid-980	FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing	link link
ETid-1094	IRELAND	2022-03-15	17,000,000	Meta Platforms Ireland Limited	Art. 5 (2) GDPR, Art. 24 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-1578	IRELAND	2023-01-19	5,500,000	WhatsApp Ireland Ltd.	Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Insufficient legal basis for data processing	link link

	ETId-1696	 IRELAND	2023-02-27	750,000	Bank of Ireland 365	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-1115	 IRELAND	2022-04-05	463,000	Bank of Ireland	Art. 32 GDPR, Art. 33 GDPR, Art. 34 GDPR	Insufficient technical and organisational measures to ensure information security	link link
	ETId-1666	 IRELAND	2023-01-23	460,000	Centric Health Ltd.	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1) GDPR	Non-compliance with general data processing principles	link
	ETId-485	 IRELAND	2020-12-15	450,000	Twitter International Company	Art. 33 (1), (5) GDPR	Insufficient fulfilment of data breach notification obligations	link
	ETId-1009	 IRELAND	2021-12-09	110,000	Limerick City and County Council	Art. 13 GDPR, Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects rights	link link
	ETId-1564	 IRELAND	2022-12-22	100,000	VIEC Limited	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Non-compliance with general data processing principles	link link
	ETId-689	 IRELAND	2021-03-23	90,000	Irish Credit Bureau DAC	Art. 5 (2) GDPR, Art. 24 (1) GDPR, Art. 25 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-570	 IRELAND	2020-08-12	85,000	Tusla Child and Family Agency	Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-278	 IRELAND	2020-05-17	75,000	Tusla Child and Family Agency	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing	link
	ETId-552	 IRELAND	2020-12-17	70,000	University College Dublin	Art. 5 (1) e), f) GDPR, Art. 32 (1) GDPR, Art. 33 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-449	 IRELAND	2020-08-18	65,000	Cork University Maternity Hospital	Art. 5 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-987	 IRELAND	2021-12-02	60,000	Irish Teacher Council	Art. 5 (1) GDPR, Art. 32 (1) GDPR, Art. 33 GDPR	Insufficient technical and organisational measures to ensure information security	link
	ETId-203	 GERMANY	2019	51,000	Facebook Germany GmbH	Art. 37 GDPR	Insufficient involvement of data protection officer	link
	ETId-320	 IRELAND	2020-06-30	40,000	Tusla Child and Family Agency	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations	link

GDPR Enforcement Tracker

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and penalties](#). Please note that we do not list any fines imposed under national / non-European laws (with the exception of fines under the UK GDPR), under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show: 25  entries

Search:

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
 ETid-1965	 IRELAND	2023-06-16	22,500	Irish Departement of Health	Art. 5 (1) c) GDPR, Art. 6 (1), (4) GDPR, Art. 9 (1) GDPR	Non-compliance with general data processing principles	link
 ETid-1677	 IRELAND	2022-12-30	15,000	A&G Couriers Limited T/A Fastway Couriers (Ireland)	Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
 ETid-1519	 IRELAND	2022-01-26	5,000	Slane Credit Union Ltd.	Art. 5 (1) f) GDPR, Art. 24 GDPR, Art. 28 (1), (3) GDPR, Art. 30 (1) GDPR, Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
 ETid-893	 IRELAND	2021-08-20	1,500	MOVE Ireland	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link link
 ETid-825	 IRELAND	2021-09-07	1,400	Vodafone Ireland Limited	Art. 21 GDPR	Insufficient fulfilment of data subjects rights	link

Compliance



Fundamental Principles



Personal Data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with subject's rights
7. Kept secure
8. Not transferred to countries without adequate protection

Your Obligation as Committee Members

- Ensure and maintain a high degree of privacy and confidentiality with regard to all Club Members' personal data
- **Prevent Data Breaches**
If / when they do occur, notify UL Studentlife asap - be mindful of mandatory 72 hour reporting requirement
- **Understand your obligations with regard to Subject Access Requests**
Requests - complete disclosure - max one month timeline from first receipt to notification





ACCESS
DENIED



Data Breach

try again

[click here for more information](#)



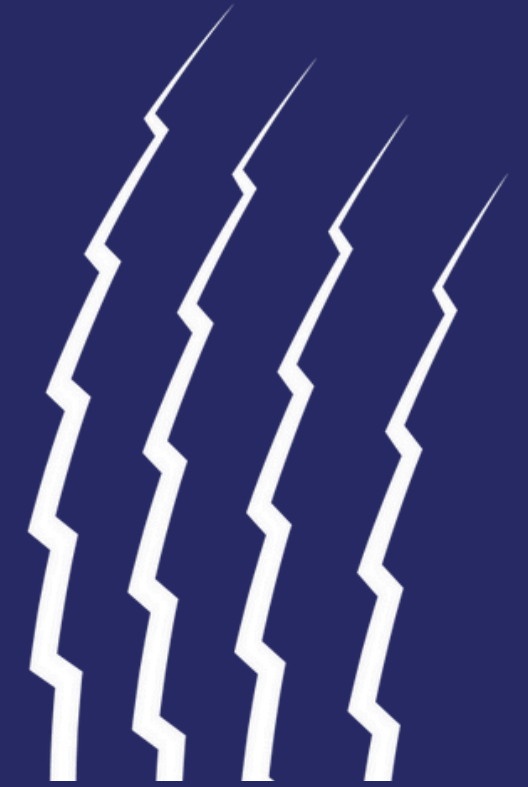
Data Breach Definition

Although the term "data breach" is not specifically defined in the Directive, Art.17(1) obliges controllers to:

Protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing.

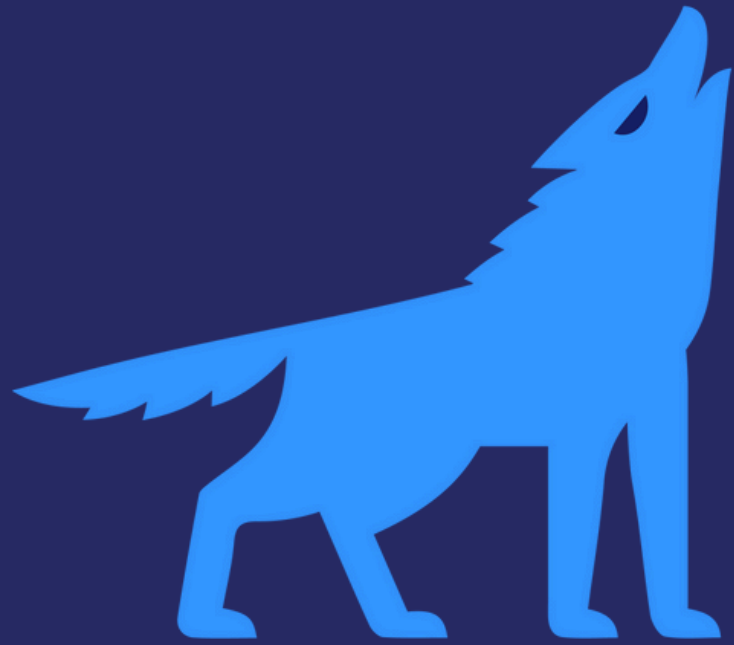


Breach Notification



- Personal Data Breach of security leading to:
 - Destruction
 - Loss
 - Alteration
 - Unauthorised disclosure or Access
- Supervisory Authority notification required where risk to rights and freedoms of individual is likely i.e. detrimental effect
- Individual notification required where a high risk to rights and freedoms of individuals is likely
- 72 hours from becoming aware to notification

Subject Access Request



- A request is valid if it is clear that the individual is asking for their personal data
 - Letter
 - Email
 - Phonecall ((although normal to request submission of follow-up in writing)
- Scope - wide ranging: “personal data relating to an identifiable individual whether provided by the data subject or not”
- Timeline - max one calendar month from receipt of initial request

C&S Committees

Be acutely aware of responsibilities and obligations associated with processing data.

Understand Obligations in relation to :

- Data Breaches
- Subject Access Requests

If in doubt..ASK



Closing Thoughts...



...Treat people's data in the way you would like others to treat your own.

Questions?

