



**Trinity College Dublin**  
Coláiste na Tríonóide, Baile Átha Cliath  
The University of Dublin

## **Trinity Business School**

# **4. Policy**

## **4.1 The Basics of GDPR**

# The 7 principles of data protection



### LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.



### STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.



### PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.



### DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.



### INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.



### ACCURACY

Personal data shall be accurate and, where necessary, kept up to date.



### ACCOUNTABILITY

The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles.

### The 8 data privacy rights of customers



#### RIGHT TO BE INFORMED

Be transparent in how you collect and process personal information and the purposes that you intend to use it for. Inform your customer of their rights and how to carry them out.



#### RIGHT OF ACCESS

Your customer has the right to access their data. You need to enable this either through business process or technical means.



#### RIGHT TO RECTIFICATION

Your customer has the right to correct information that they believe is inaccurate.



#### RIGHT TO ERASURE

You must provide your customer with the right to be forgotten, provided that your legitimate interest to hold such information does not override theirs.



#### RIGHT TO RESTRICTION OF PROCESSING

Your customer has the right to request that you stop processing their data.



#### RIGHT TO DATA PORTABILITY

You need to enable the machine and human-readable export of your customers' personal information.



#### RIGHT TO OBJECT

Your customer has the right to object to you using their data.



#### RIGHTS REGARDING AUTOMATED DECISION MAKING

Your customer has the right not to be subject to a decision based solely on automated processing, including profiling.

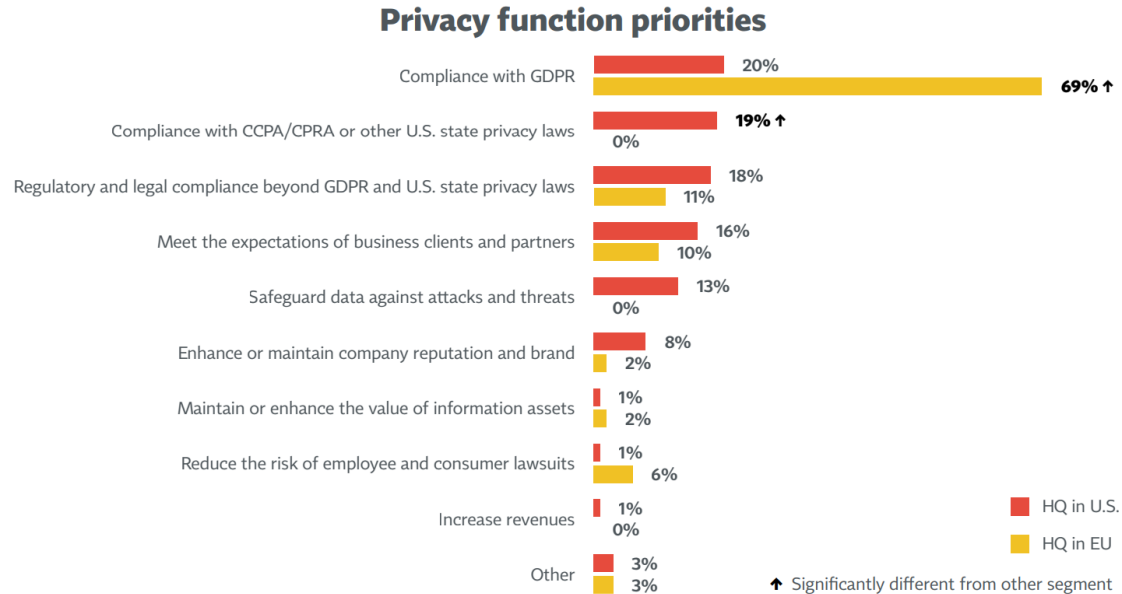
### In-class discussion

**Based on the reading of the text „Privacy Issues and Data Protection in Big Data” and your personal notes, how do you answer the following questions:**

How did the GDPR impact the 2 research projects?

What are the key challenges associated with GDPR-compliant data processing and analysis?

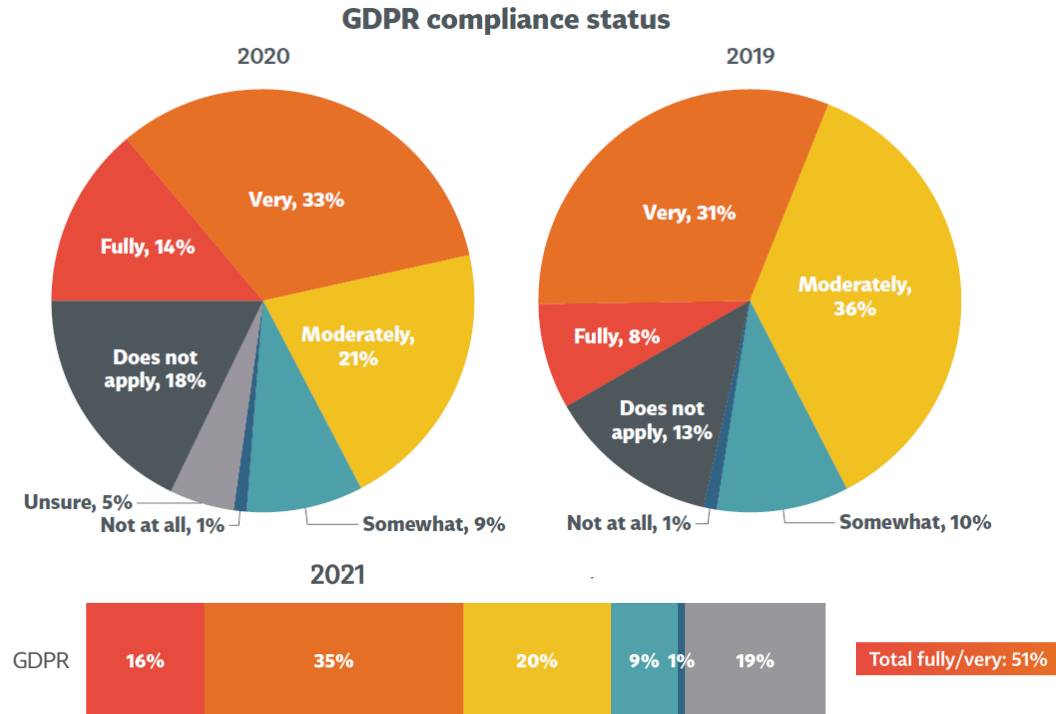
# GDPR has become a top priority for privacy professionals



Source: IAPP-FTI Consulting Privacy Governance Report 2021.

## 4.2 The Impact of GDPR

### The current status of GDPR compliance



#### BY HQ LOCATION

	U.S.	EU
Level of GDPR compliance		
Fully compliant	16%	12%
Very compliant	29%	45%
Moderately compliant	19%	27%
Somewhat compliant	6%	15%
Not at all compliant	1%	0%
GDPR doesn't apply	23%	0%

Significantly different than other segment

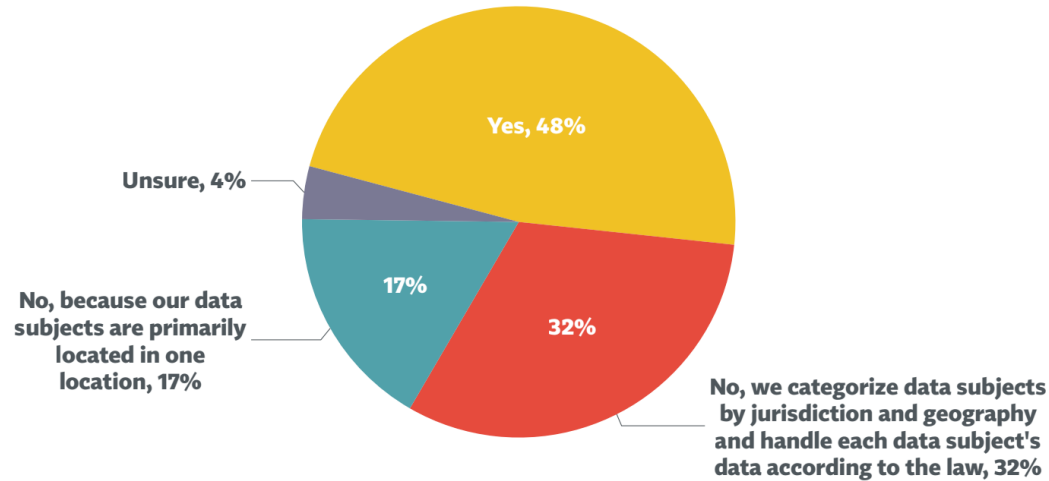
**NET "FULLY/VERY"  
COMPLIANT**

**U.S.: 45%**  
**EU: 57%**

Source: IAPP-FTI Consulting Privacy Governance Report 2020+2021.

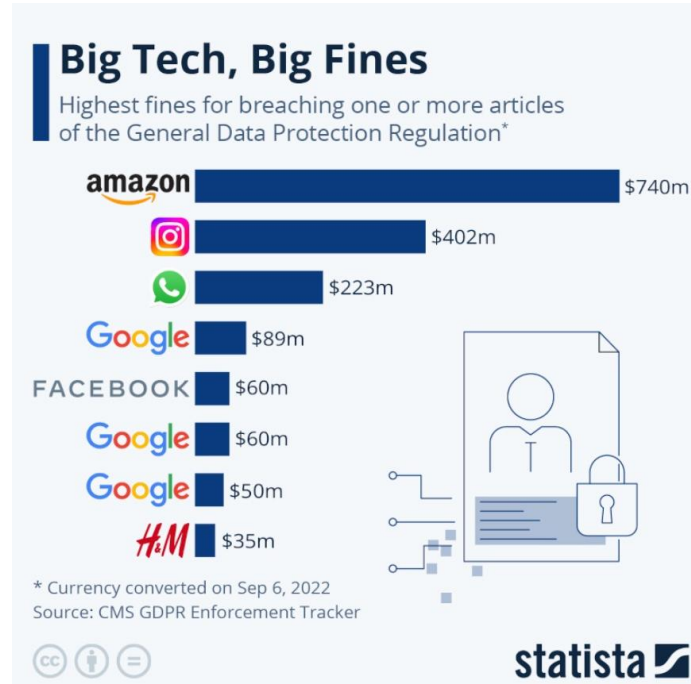
### Trend towards global standardization

Does your organization have a single global data protection/privacy strategy for data subjects' rights?



Source: IAPP-FTI Consulting Privacy Governance Report 2021.

# Overview of outcomes from enforcing GDPR in EU



Source: Statista, CMS GDPR Enforcement Tracker, 2022.



### Enforcement I: The French GDPR fine for Google „Forced consent“



- Google received a 50 Mio. € fine by the French DPA for violating GDPR rules in 2019 in relation to transparency and consent when setting up a new Android device
- Google had not provided clear enough information for consent to be lawfully obtained
- For consent to be a valid legal basis for processing personal data it must be informed, specific and freely given

### Enforcement II: The German GDPR fine for H&M



- H&M Germany received a €35.2 million fine in 2020 for the excessive monitoring of several hundred employees by one of the clothing retailer's German subsidiaries
- After employee absences, including vacations and sick leave, supervising team leaders would conduct so-called “Welcome Back Talks” with the employees, and then would record details of those conversations that included their holiday experiences, symptoms of illness, and diagnoses.
- In addition to a meticulous evaluation of individual work performance, the data collected in this way was used, among other things, to obtain a detailed profile of employees for measures and decisions regarding their employment.

### Enforcement III: The Irish DPC and Meta



- Meta Platforms Inc. (Instagram) received a 405 Mio. € fine by the Irish DPC for violating GDPR rules in 2022 in relation to the processing of personal data of minors and their privacy
- WhatsApp Ireland Inc. received a fine of 225 Mio. € in 2021 for failing to sufficiently inform users about how their data is processed
- The GDPR's consistency mechanism (coined 'one-stop shop') requires that the supervisory authority in the Member State where a company has declared its main establishment takes the lead on all privacy related matters

### Overview of important effects of the GDPR

- Changing the regulatory landscape of data protection on a global scale
- Increased staff in the privacy and data protection area
- Enforcement agencies are overwhelmed with scope and complexity of enforcing the GDPR
- High costs and lack of support for SMEs (EU offers useful [GDPR checklist](#))