UNIVERSITÉ CÔTE D'AZUR

Inria INVENTEURS DU MONDE NUMÉRIQUE

GDPR rights

Nataliia Bielova

@nataliabielova

Privacy, Security and ethical aspects of data

Université Cote d'Azur

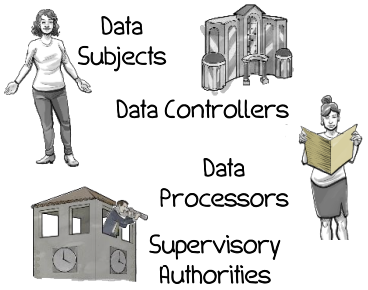
GDPR

TERRITORIAL SCOPE

EU Establishments

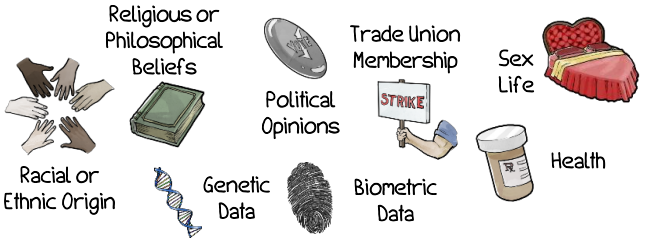
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA

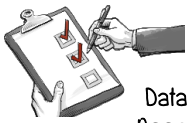
SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

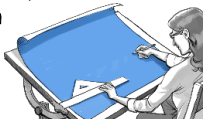
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.



Data Impact Assessment
For high risk situations

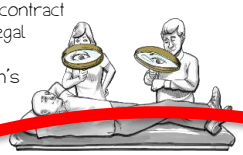
Data Protection by Design
built in starting at the beginning of the design process



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

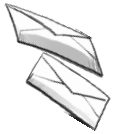
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

Consent must be freely given, specific, informed, and unambiguous.

DATA BREACH NOTIFICATION

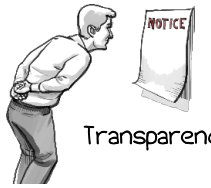


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

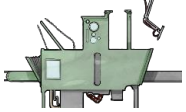
Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



"Right not to be subject to a decision based solely on automated processing, including profiling."

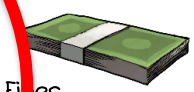
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT



Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY 2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

RIGHTS OF DATA SUBJECTS

Rights of the Data Subject

- Individuals have rights to keep control of their personal data.
- Data Controller (DC) should be able to explain how to exercise their rights.
- Once an individual exercises her right, DC has to respond within 1 months

GDPR

Chapter 3

Rights of the data subject

To implement these rights, a data controller must authenticate data subjects first!

Section 1	–	**Transparency and modalities**
Article 12	–	Transparent information, communication and modalities for the exercise of the rights of the data subject
Section 2	–	**Information and access to personal data**
Article 13	–	Information to be provided where personal data are collected from the data subject
Article 14	–	Information to be provided where personal data have not been obtained from the data subject
Article 15	–	Right of access by the data subject
Section 3	–	**Rectification and erasure**
Article 16	–	Right to rectification
Article 17	–	Right to erasure ('right to be forgotten')


GDPR
The General Data Protection Regulation
YOU HAVE THE RIGHT....
not to remain silent. :)

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing

The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

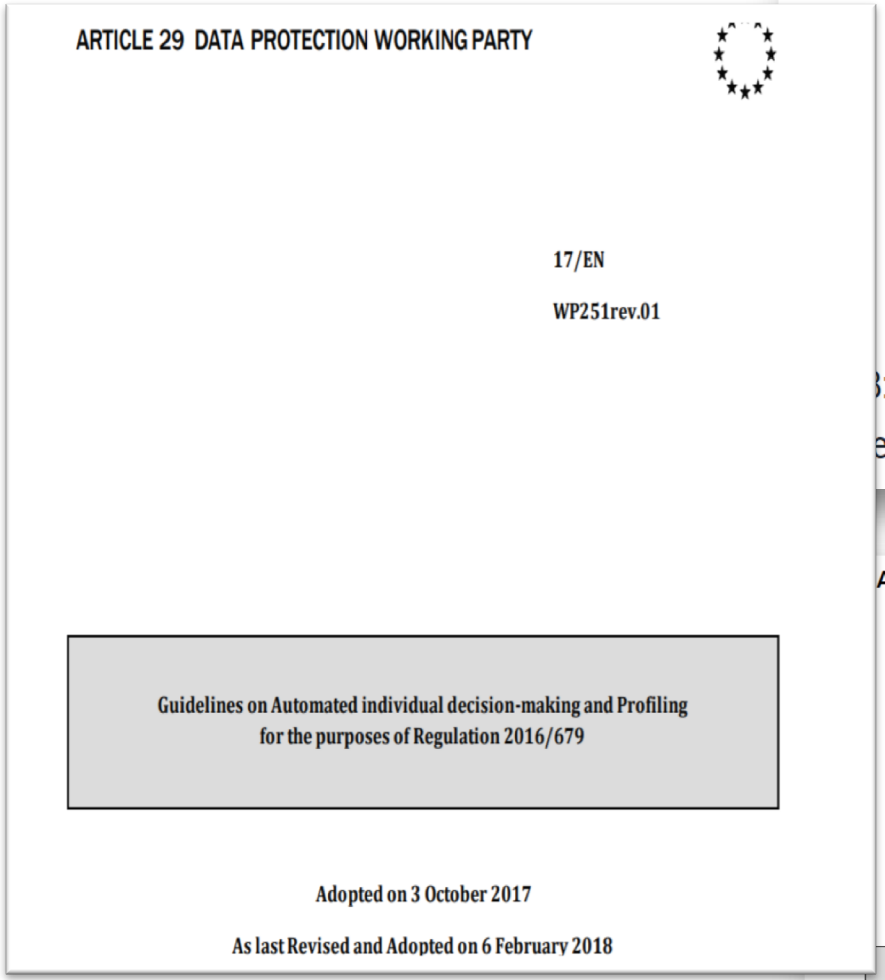
This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.


ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP251rev.01

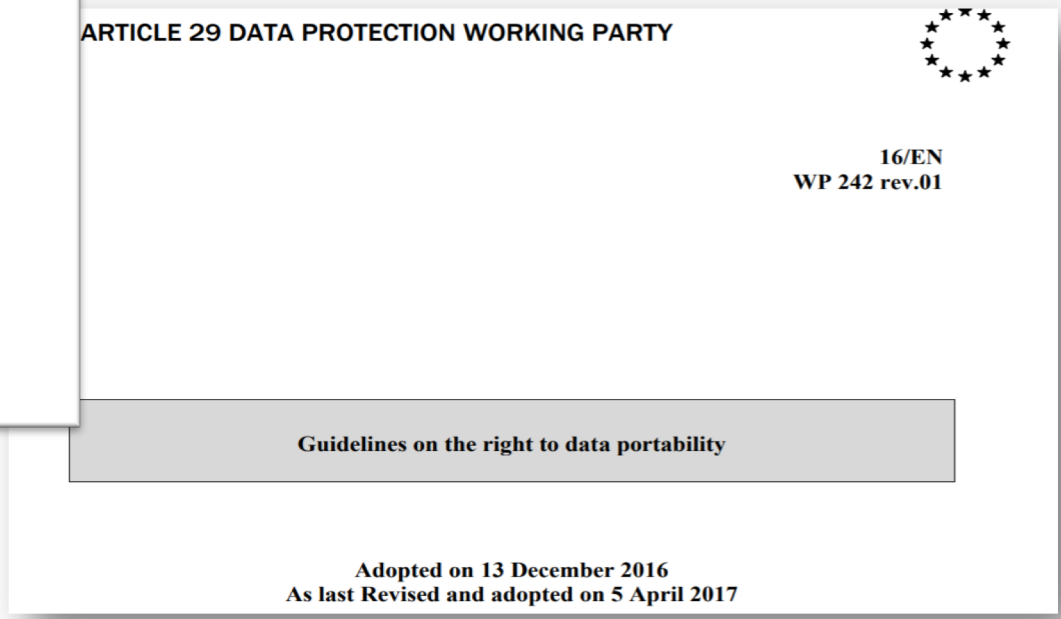
Guidelines on Automated individual decision-making and Profiling
for the purposes of Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

European Data Protection Board

: Guidelines 5/2019 on the criteria of the Right to be Forgotten in
earch engines cases under the GDPR


ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 242 rev.01

Guidelines on the right to data portability

Adopted on 13 December 2016
As last Revised and adopted on 5 April 2017

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing

The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

Right to be informed, Art. 13, 14

DS need to know who, what, how to exercise control on her data

CLEAR

concise, transparent, intelligible and easily accessible form, using clear and plain language

Free of charge

Right to be informed

Timeframe

- If data is **collected directly** from the DS, e.g. filled a form
  - When the data is collected from him
- If data is **not collected directly** from the DS, e.g. transferred from other controller
  - Within a reasonable time (max. 1 month) of the collection
  - If the data are collected to communicate with a DS or to transmit the data to another controller, during the first communication with the data subject / to the new controller

Exceptions (direct)

- The DS already has the information

Exceptions (indirect)

- The DS already has the information
- Impossible or disproportionate effort
- Collection or disclosure foreseen by law
- Professional secrecy

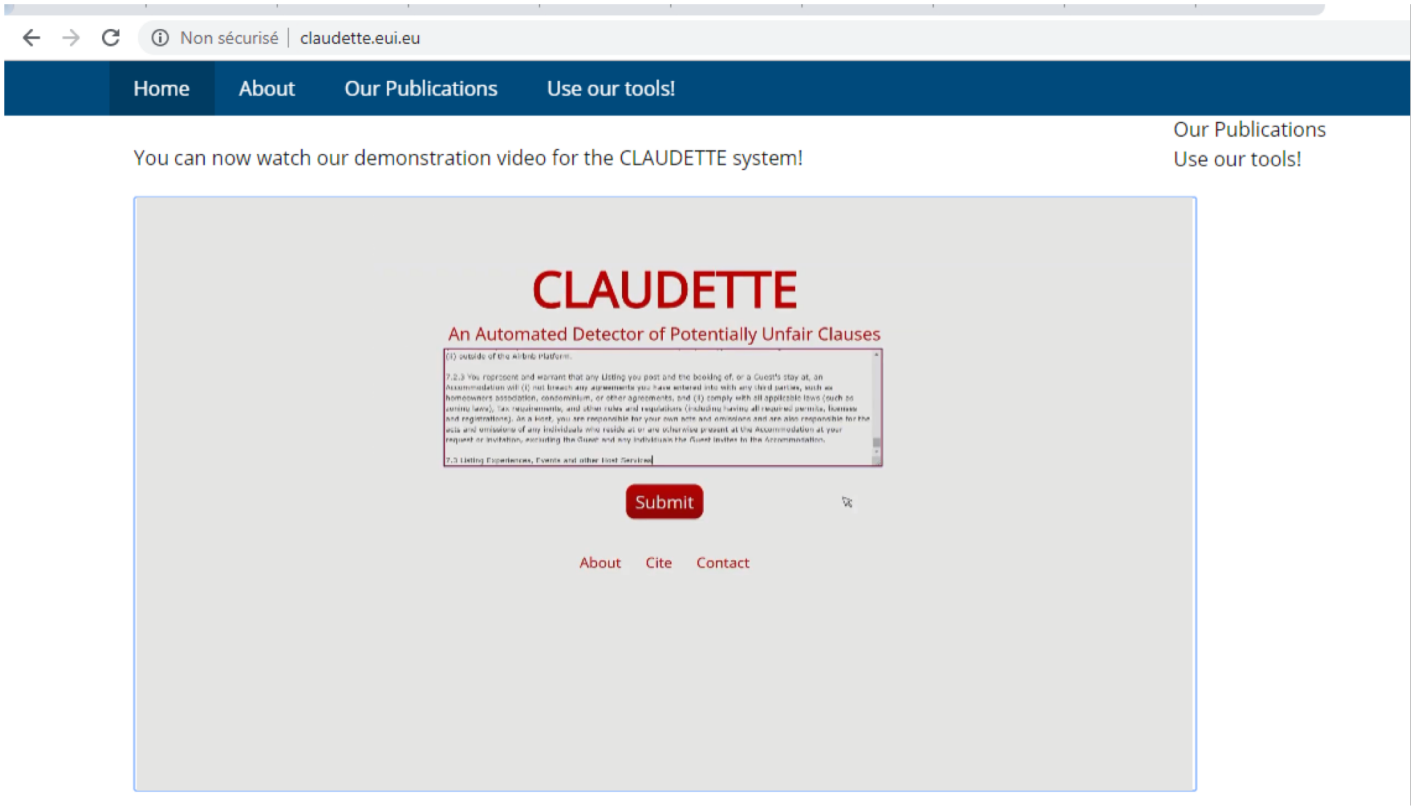
Informed of a bunch of information

The data are collected	Directly	Indirectly
The identity and contact details of the controller (& representative, if applicable)	☑	☑
The contact details of the DPO (if applicable)	☑	☑
The purposes of the processing, the legal basis for the processing and the legitimate interests (if processing is founded on legitimate interest)	☑	☑
The categories of personal data concerned		☑
The recipients or categories of recipients of the personal data	☑	☑
The transfers of personal data to third countries (including safeguards)	☑	☑
The storage duration (or, if impossible, the criteria used to determine that period)	☑	☑
The rights of the DS	☑	☑
The rights to withdraw consent (if applicable)	☑	☑
The right to lodge a complaint with a supervisory authority	☑	☑
The source of the personal data (incl. if from publicly accessible sources)		☑
If there is a statutory or contractual requirement to provide the data, if the provision of the personal data is obligatory & possible consequences of a refusal	☑	
If automated decision-making, incl. profiling, is used (if so, meaningful information about the logic, significance & envisaged consequences for the DS)	☑	☑
Further processing of the personal data	☑	☑

Legal Design

Privacy Policies

Machine Learning Powered Analysis of Consumer Contracts and Privacy Policies



The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

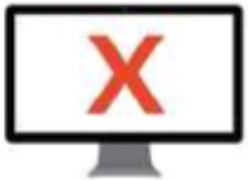
You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing



The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

Right of access:

"You know way too much about me... What do you have on me? Art.15#59,63, 64

Elements

1) Check if data is being processed about her: awareness
2) Check ii. lawfulness of processing; ii. quality/accuracy of her own data
3) Informed about:
   - Purposes
   - categories of personal data concerned
   - 3° Parties recipients
   - Storage duration
   - DS rights, incl. the right to lodge a complaint with a DPA
   - Source of the personal data (if collected indirectly)
   - If automated decision-making, incl. profiling, is used (if so, meaningful information about the logic behind, the significance & consequences)

4) right to receive a (free) copy of the personal data

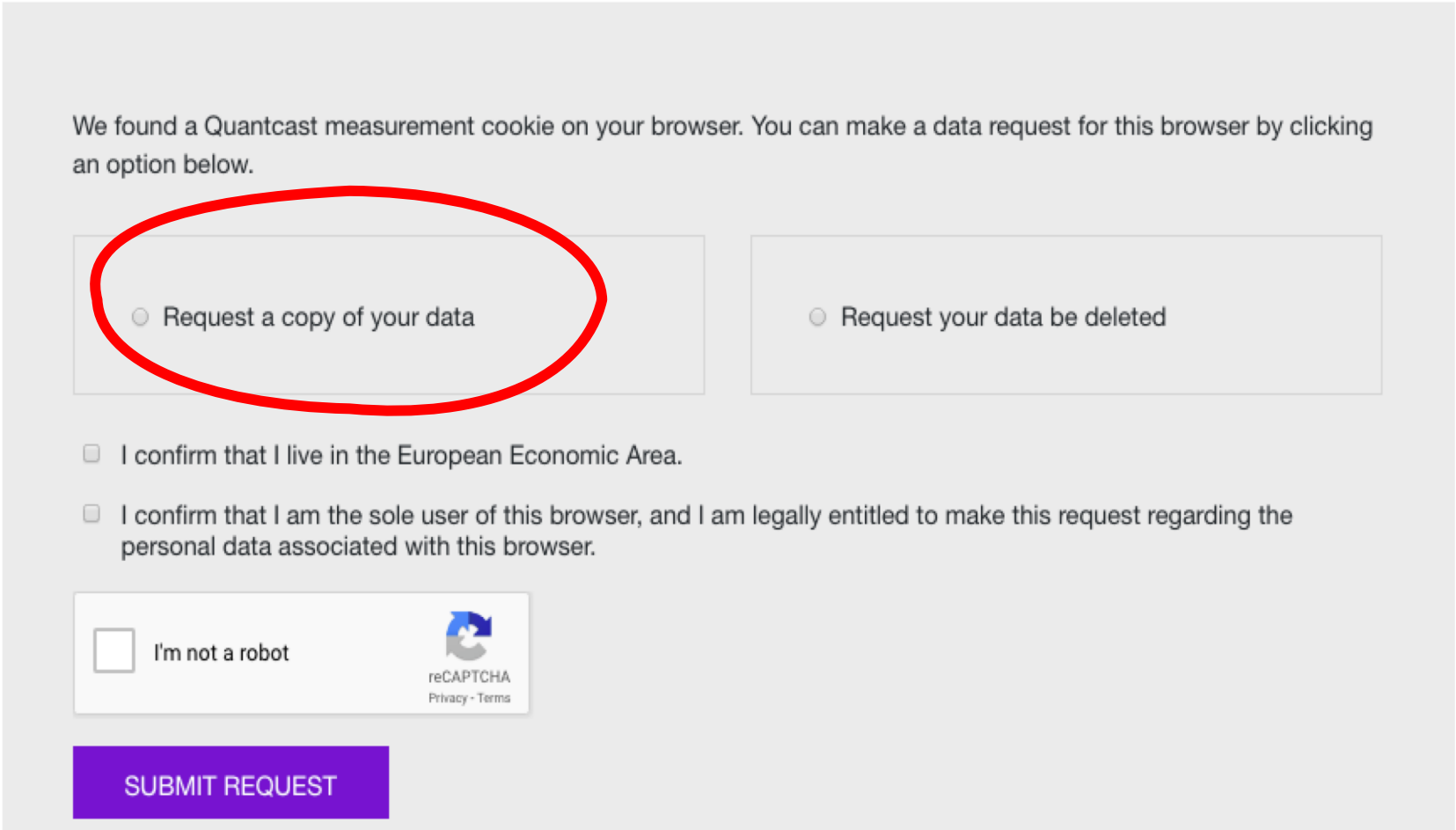
Timeframe

- Without undue delay,
- within **1 month** of the request (possible extension of 2 months)

Exceptions

- The right shall not adversely affect the rights of others
- #63 protection of intellectual property rights and trade secrets (eg. if release of logic of automated decision taking would involve release of such information)

Right to Data Request Form



Case C-434/16, Nowak v DPC

- Trainee accountant failed one accountancy exam 4 x
- Questioned the 4th result, then requested access to all PD held by the accountancy body, the CAI
- Received 17 items, but not the exam script, not "PD"
- Asked Irl DPA for help, which concluded that not PD
- Challenged DPA decision before cts, Supreme Court asked CJEU **whether exam script is PD** and what factors are relevant in concluding whether it is PD
- Q also raised before CJEU whether examiner's corrections to a script also constitute personal data
- Cf Joined Cases C-141/12 and C-372/12, *YS and Others*, 17 July 2014

- As regards the latter condition [i.e. relates to], it is satisfied where the information, by reason of its content, purpose or effect, is **linked** to a particular person.
- Exam scripts/Examiner's comments
  - Content – reflects extent of the candidate's knowledge
  - Purpose – evaluate candidate's knowledge and professional suitability
  - Result – may determine whether he can enter the profession

Concept	Simplified definition
Right of access	The data subject has the right to access the data (original, processed and derived data) that a controller has on him/her and to obtain a copy of that data (original, processed and derived data). E.g. the right to know all the information that your bank has on you and obtain a copy of them, even of the derived data.
Original data	The personal data provided by the data subject. E.g. the data you give by filling a form when you enter into a contract, but even simply the e-mail address you give when you sign up for a service
Processed data	The personal data after they have been processed by the controller, thus after they have been stored, organised, structured, modified, combined, etc.
Derived data	The inferred and derived data generated by the controller from the analysis of the original data e.g. when the controller profiles or classifies a person according to his purchase pattern, assigns him a (credit) score

Data subject rights vs Data controller fears

Data Subject

Data Controller

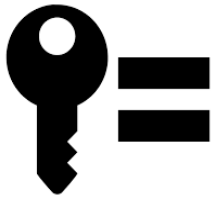
- How do I exercise my access right?
- How do I prove my identity to the controller?
- Can other person **impersonate** me? (use my credentials to get my data)
- Will they do **abusive identity check**? (ask me for more than necessary, or irrelevant docs)

- Is this request legitimate?
- What is necessary to identify this person's data?
- What if the data subject is illegitimate?
- What if I release the data from Réka to Leon?

And if there are doubts about the identity of the DS?

If the PD the DC has is not sufficient to identify a person, the DC should **not be obliged to acquire additional information in order to identify the** DS, for the sole purpose of compliance

But… if the user gives his PD to support his access right, the controller should not refuse to take it



Identification= through the same credentials used by DS to login to the online service offered by the controller

Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data

Coline Boniface [1] , Imane Fouad [2] , Nataliia Bielova [2] , Cédric Lauradoux [1] , Cristiana Santos [3] Details

1 PRIVATICS - Privacy Models, Architectures and Tools for the Information Society
Inria Grenoble - Rhône-Alpes, CITI - CITI Centre of Innovation in Telecommunications and Integration of services

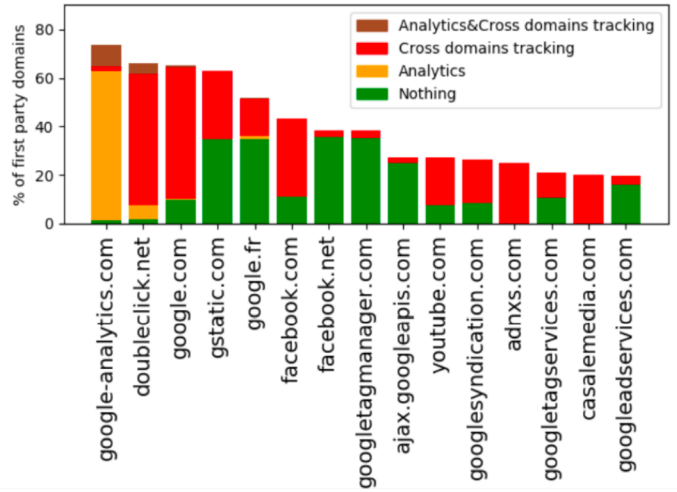
2 INDES - Secure Diffuse Programming
CRISAM - Inria Sophia Antipolis - Méditerranée

3 UT1 - Université Toulouse 1 Capitole

Abstract : With the GDPR in force in the EU since May 2018, companies and administrations need to be vigilant about the personal data they process. The new regulation denes rights for data subjects and obligations for data controllers but it is unclear how subjects and controllers interact concretely. This paper tries to answer two critical questions: is it safe for a data subject to exercise the right of access of her own data? When does a data controller have enough information to authenticate a data subject? To answer these questions, we have analyzed recommendations of Data Protection Authorities and authentication practices implemented in popular websites and third-party tracking services. We observed that some data controllers use unsafe or doubtful procedures to authenticate data subjects. The most common flaw is the use of authentication based on a copy of the subject's national identity card transmitted over an insecure channel. We define how a data controller should react to a subject's request to determine the appropriate procedures to identify the subject and her data. We provide compliance guidelines on data access response procedures.

https://hal.inria.fr/hal-02072302

Exercising SAR on 30 popular third-party trackers



No response or not possible to contact	4
Not able to get information on how to exercise SAR before we give the data	2
Deny access to third-party data	7
Use third-party cookies as online identifier	12
Require copy of an ID card	4
Direct access without any additional info	2

We identified 25 companies that own top 30 third-party tracking domains

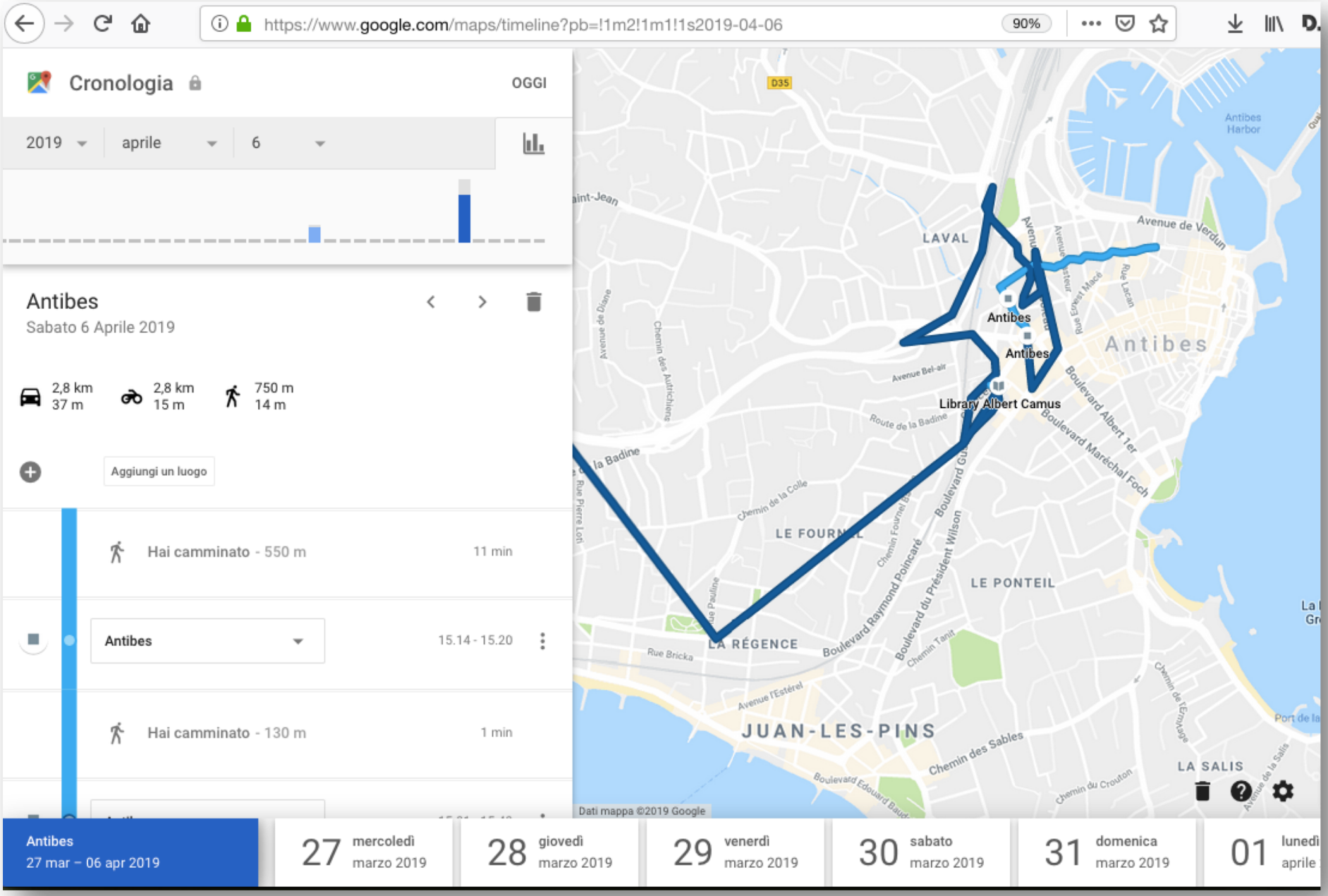
Exercise your own right now!

Exercise!

Exercise 1: Your location

- Google stores your location (if you have it turned on) every time you turn on your phone, and you can see a timeline from the first day you started using Google on your phone

- Open your Google location history:
- https://www.google.com/maps/timeline?pb


https://www.google.com/maps/timeline?pb=!1m2!1m1!1s2019-04-06
90%
Cronologia
OGGI
2019
aprile
6
Antibes
Sabato 6 Aprile 2019
2,8 km
37 m
2,8 km
15 m
750 m
14 m
Aggiungi un luogo
Hai camminato - 550 m
11 min
Antibes
15.14 - 15.20
Hai camminato - 130 m
1 min
Antibes
27 mar – 06 apr 2019
27 mercoledì marzo 2019
28 giovedì marzo 2019
29 venerdì marzo 2019
30 sabato marzo 2019
31 domenica marzo 2019
01 lunedì aprile
Dati mappa ©2019 Google
LAVAL
Antibes
Library Albert Camus
LE FOURNEL
LE PONTEIL
LA RÉGENCE
JUAN-LES-PINS
LA SALIS
Boulevard Albert 1er
Boulevard Maréchal Foch
Boulevard du Président Wilson
Boulevard Raymond Poincaré
Chemin des Sables
Avenue de Verdun
Route de la Badine
Avenue Bel-air
Antibes Harbor

Exercise!

Exercise 2: Your activity

- Google stores search history across all your devices on a separate database

- Open your Google activity:
  - https://myactivity.google.com/myactivity

Exercise!

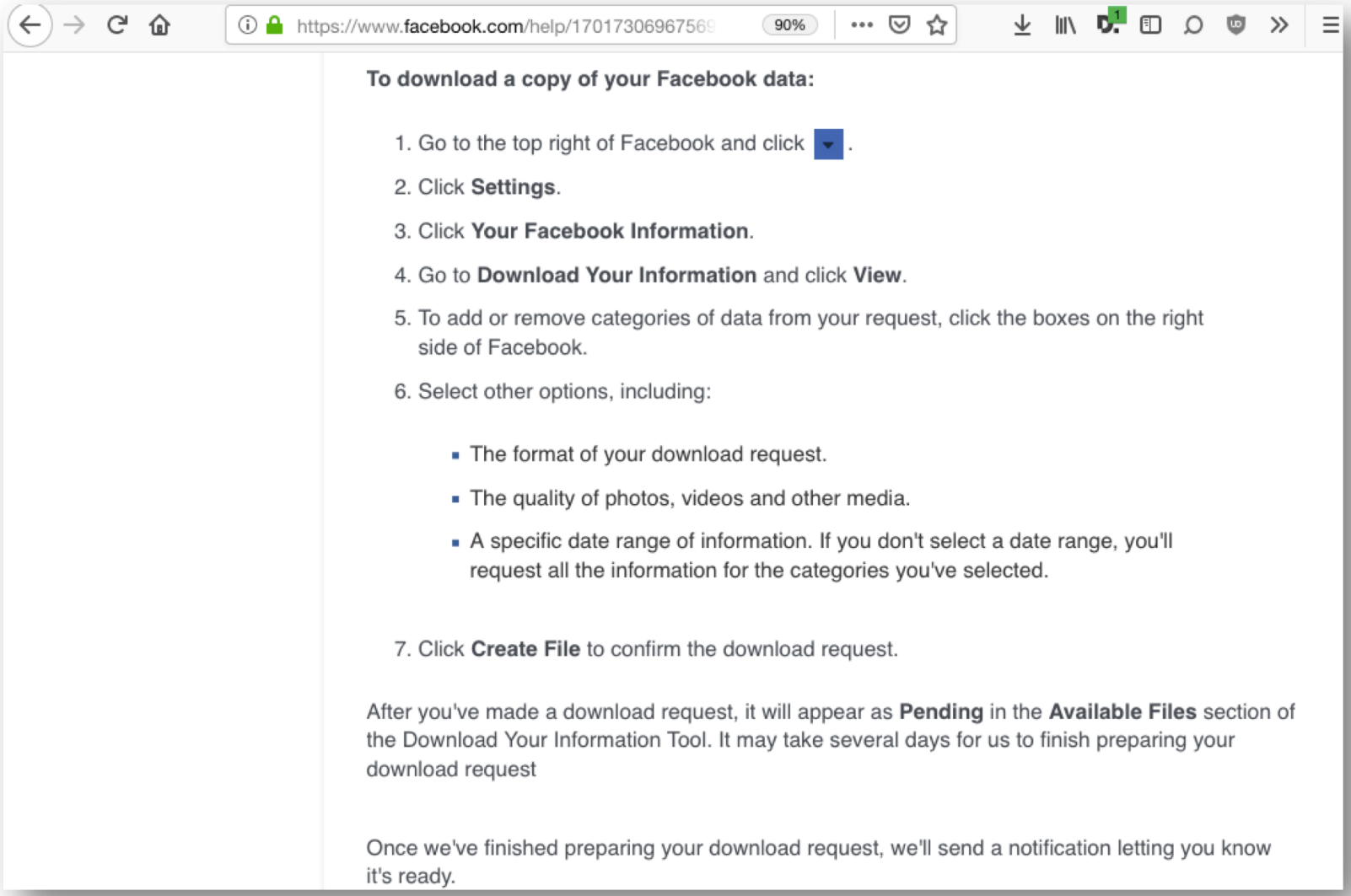
More exercises for Google

- Google advertisement profile:
  - http://www.google.com/settings/ads/
- App and extensions permissions:
  - https://myaccount.google.com/permissions/?pli=1
- Youtube history:
  - https://www.youtube.com/feed/history/search_history

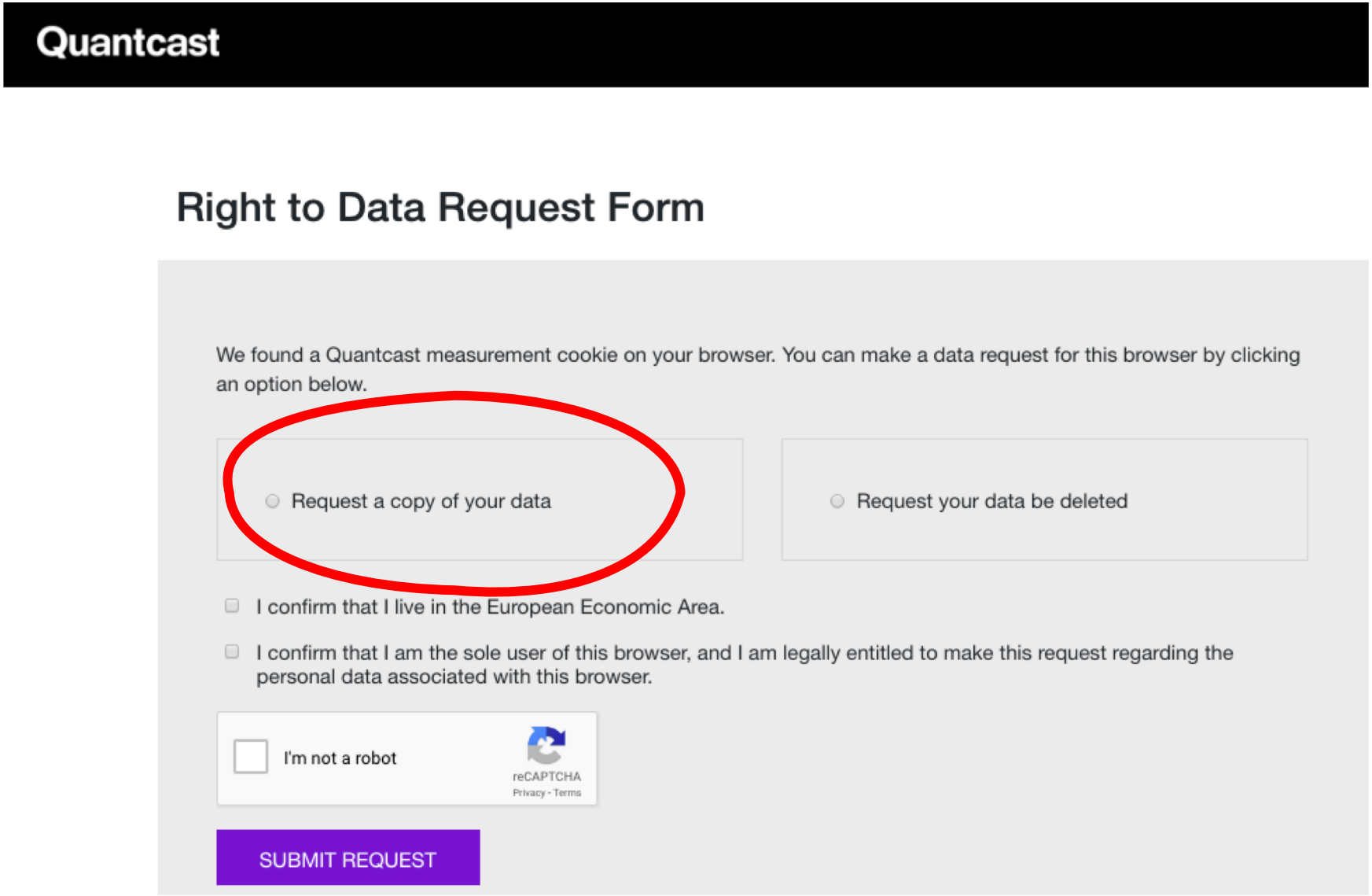
- All the data Google stores about you:
  - https://takeout.google.com/settings/takeout

Facebook

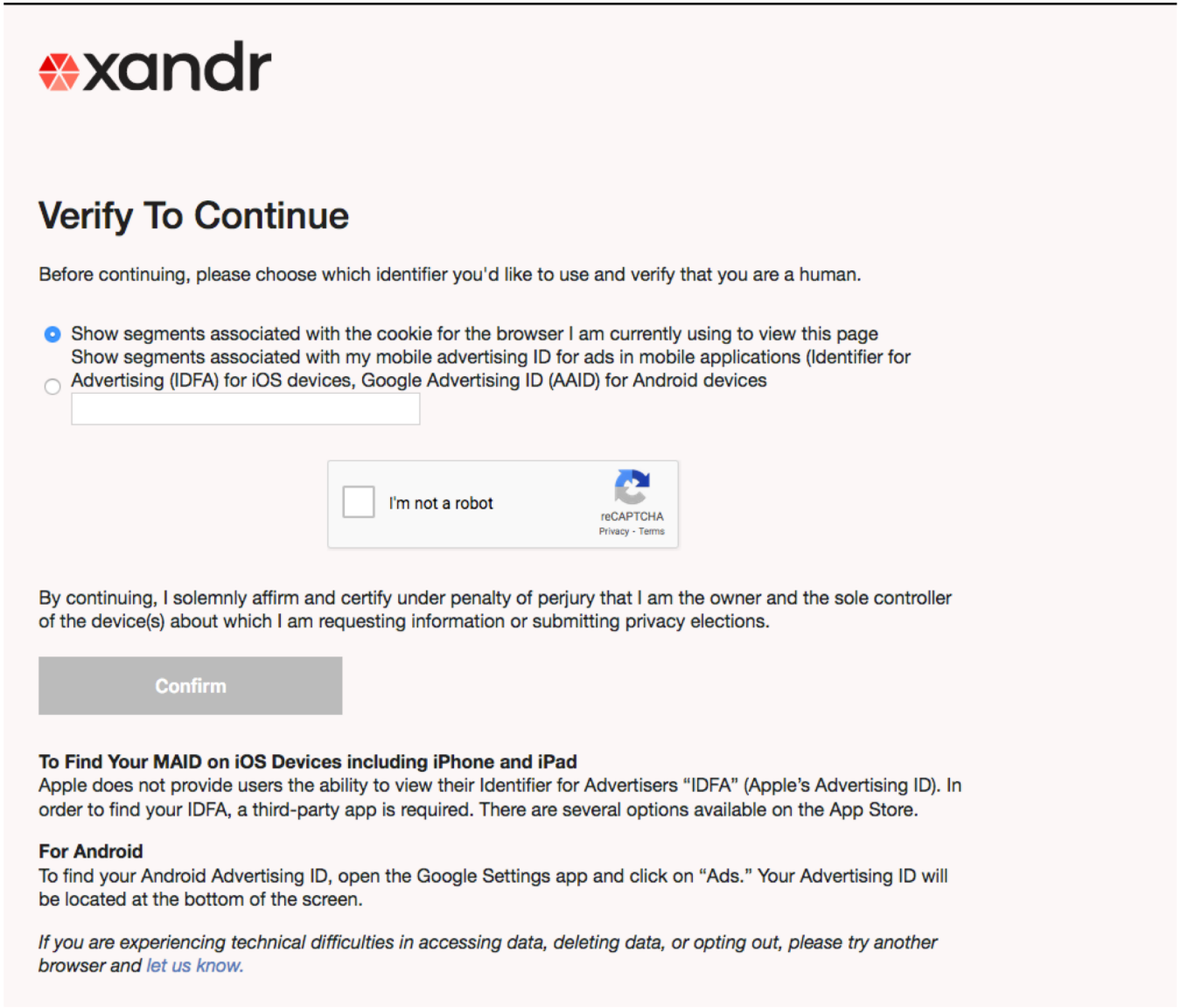
https://www.facebook.com/help/1701730696756992



https://www.quantcast.com/privacy/data-subject-rights/



https://platform.xandr.com/privacy-center/captcha?next_page=/privacy-center/access



The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing

The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

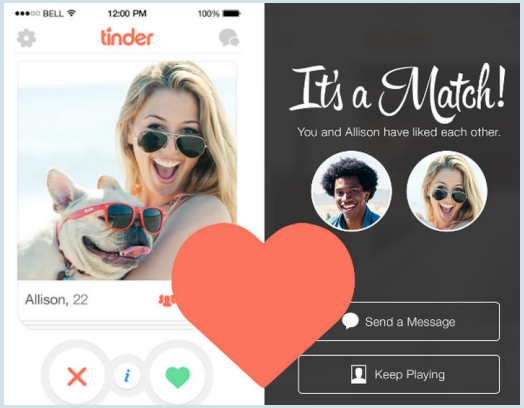
Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

data quality

Right to rectification? Art.16#65

Elements

- Right to obtain the correction or completion of personal data
  - Inaccurate data => rectification of data
  - Incomplete data => completion



Cristiana Santos, Utrecht University

Timeframe

- Without undue delay and in any event within **1 month** of the request (possible extension of 2 months)

Notification

- Obligation to notify the rectification to each recipient to whom the data have been disclosed (unless impossible or disproportionate effort)
- Obligation to inform the DS of these recipients, at the request of the latter

A reformed criminal requests Google to delete any references to his criminal past from search results

A customer requests a company to delete their data from any marketing mailing lists

An employee requests to delete a bad performance report

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

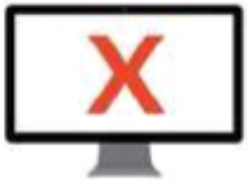
You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing



The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

Right to erasure

"right to be forgotten" Art 17#66

Which Cases

1. Data no longer necessary for the initial purposes
2. Withdrawal of consent
3. DS exercises right to object
4. Unlawful processing
5. Legal obligation requiring deletion
6. Data added to social media when the person was a child

Timeframe

- Without undue delay and in any event within **1 month** of the request (possible extension of 2 months)
- Notify any one to whom it has disclosed such data

Exceptions

- Freedom of expression and information
- Compliance with a legal obligation
- Public interest in public health
- Archiving purposes
- Legal claims

- Ex. newspaper reports public affair. Keeps records under commercial law. In case of offence, DC needs the data to start a legal claim;
- dating app still shows the profile

Refused

- None of the above conditions are fulfilled
- DS does not prove its identity
- The request is "manifestly unfounded or excessive"
- One of the exceptions of article 17(3) apply

Case “Google Spain”

In the case C-131/120, **Mario Costeja González** started legal proceedings against the editor of a Spanish newspaper (La Vanguardia SL) and against Google Spain & Google Inc. because by **searching his name in Google, he discovered articles published in that newspaper 16 years ago about his social security debts.** Mr. González said that the proceedings about him were fully resolved for several years and that reference to them was now entirely irrelevant

Right to have Google delete links to irrelevant and outdated data

Right to economic interest of a search engine, and the interests of other internet users/general public

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing

The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

Right to restrict processing

Art 18#68

Right to restriction of processing data until an accuracy dispute is verified = "*stop for now, while the situation is being analysed*"

When?

- Retention of unlawfully processed data, no longer necessary
- Retention of data for legal claims
- Accuracy & rectification is being contested by data subject
- Person objected to processing (based on legitimate interests), then requires data restriction while DC checks the legal basis

Consequences:

- Storage ok for a period
- Prohibited further processing

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing

The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

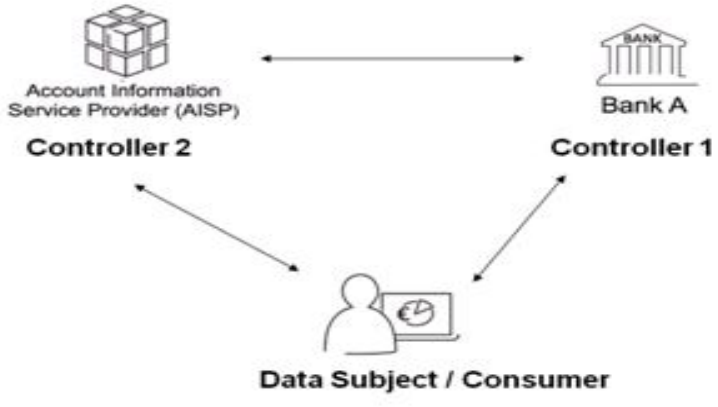
Right to data portability: "receive & reuse" Art. 20#68; WP242

Right to **receive** the PD concerning her from the DC
Right to **transmit** that data to another DC

- where technically feasible (across different services), without hindrances

Form: structured, commonly used, machine-readable and interoperable form

When: on consent/contract; by automated means



- money transferred to another bank;
- retrieving current playlist from a music streaming service;
- retrieve contact list from webmail application

Data which the individual “has provided”

data from **online forms filled in by a user**

gathered by the controller in the course of its dealings with the user

generated from **observation** of her activity

Not possible → inferred or derived data
(eg. results of an algorithmic analysis of an person’s behavior)

“
- data held by a music streaming service
- titles of books held by an online bookstore
- data from a smart meter or other connected objects
- activity logs
- history of website usage
- search activities
- emails sent to the user

”

The right to be informed

Companies will now need to include some form of privacy notice, emphasising the need for transparency over how they use your personal data.

The right of access

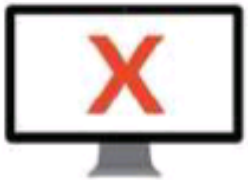
You will be able to obtain confirmation that your data is being processed, access to your personal data and other supplementary information.

The right to rectification

You are entitled to have incorrect data rectified. If it has been disclosed to third parties, companies must inform them as well as you.

The right to erasure

This allows you to request the removal of personal data where there is no compelling reason for its continued processing



The right to restrict processing

You will have the right to 'block' processing of personal data. When restricted, companies are permitted to store data, but not process it.

The right to data portability

This allows you to obtain and reuse your personal data across different services. You can move, copy or transfer data without hindrance.

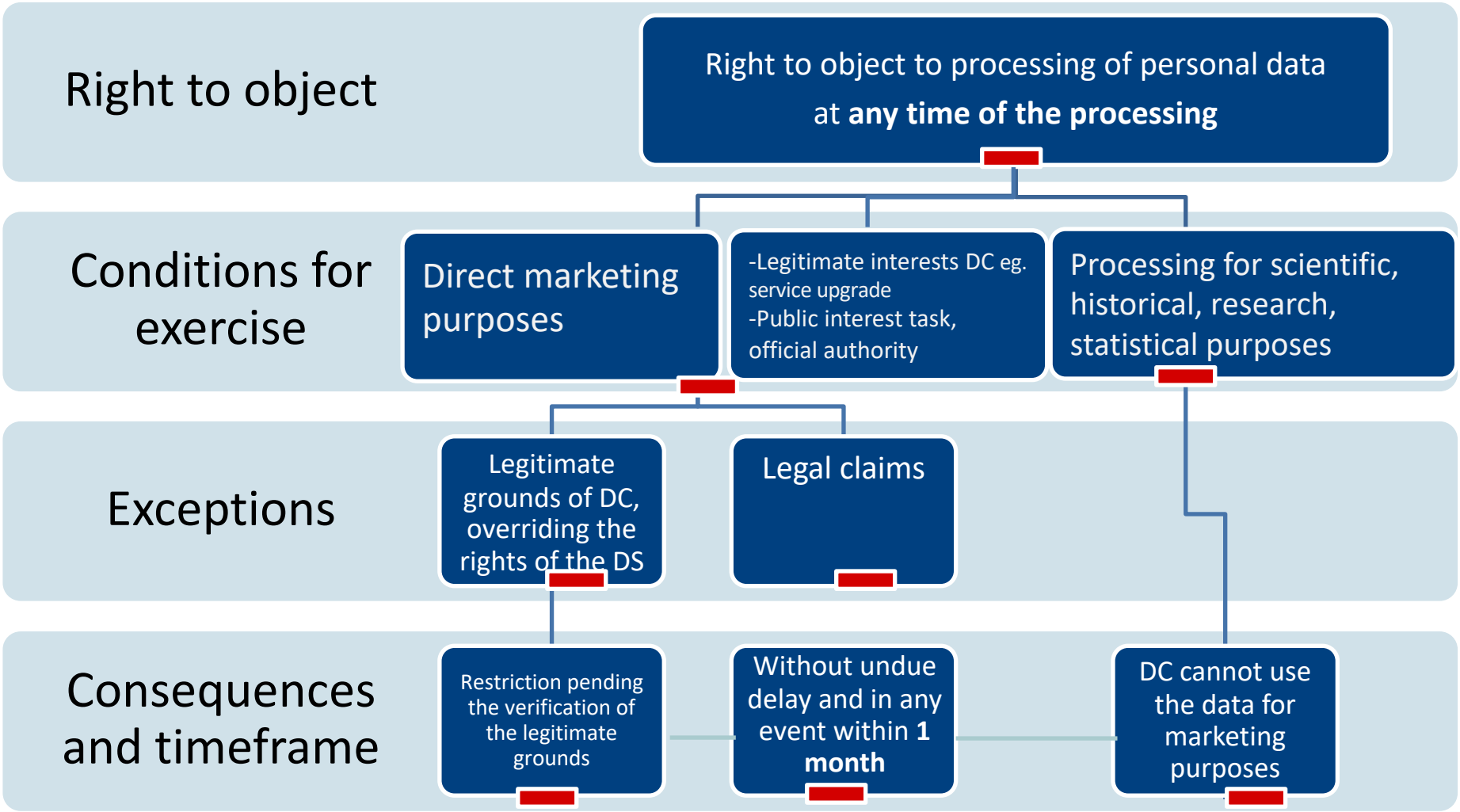
The right to object

You will be able to object to processing based on legitimate interests, direct marketing, and processing for the purpose of research and statistics.

Automated decision making & profiling rights

Safeguards are provided against the risk that a potentially damaging decision is taken without human intervention.

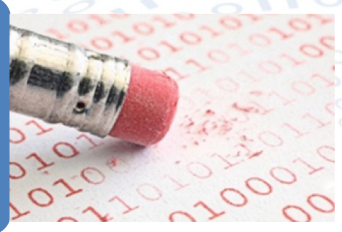
Right to object Art.21#69, 70



Right to Object v. Right to Erasure

object

erase



scope

grounds

object	erase
specific processing operations	all personal data of the DS
particular situation data subject	purpose consent lawful (-)...