GDPR

Regulating Processing of Personal Data

Harshvardhan J. Pandit
harshvardhan.pandit@dcu.ie

CA349 IT Architecture | DCU
Slides available at: https://harshp.com/research/presentations

Harsh(vardhan J. Pandit)

An Introduction

- Assistant Professor - ADAPT Centre - Dublin City University
- Postdoctoral Fellowship: knowledge graph for DPIA / GDPR
- PhD in Computer Science (2020) - Representation of activities involving personal data and consent for GDPR information
- Chair of W3C Community Groups: Data Privacy Vocabularies and Controls Community Group (DPVCG) and Consent (ConsentCG)

GDPR[1]

World-Changing EU law that regulates Processing of Personal Data

1. What is meant by Personal Data ?
2. What is meant by Processing ?
3. How is data is being processed? (what/how/where…)
4. Who is involved? (whose data, processed by whom)
5. How to check processing is following the rules of GDPR?

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Personal Data

GDPR

Personal Data

Some “definitions” from across the globe

‘personal data’ means **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;

GDPR Art.4(1)

any information that (a) **can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal**

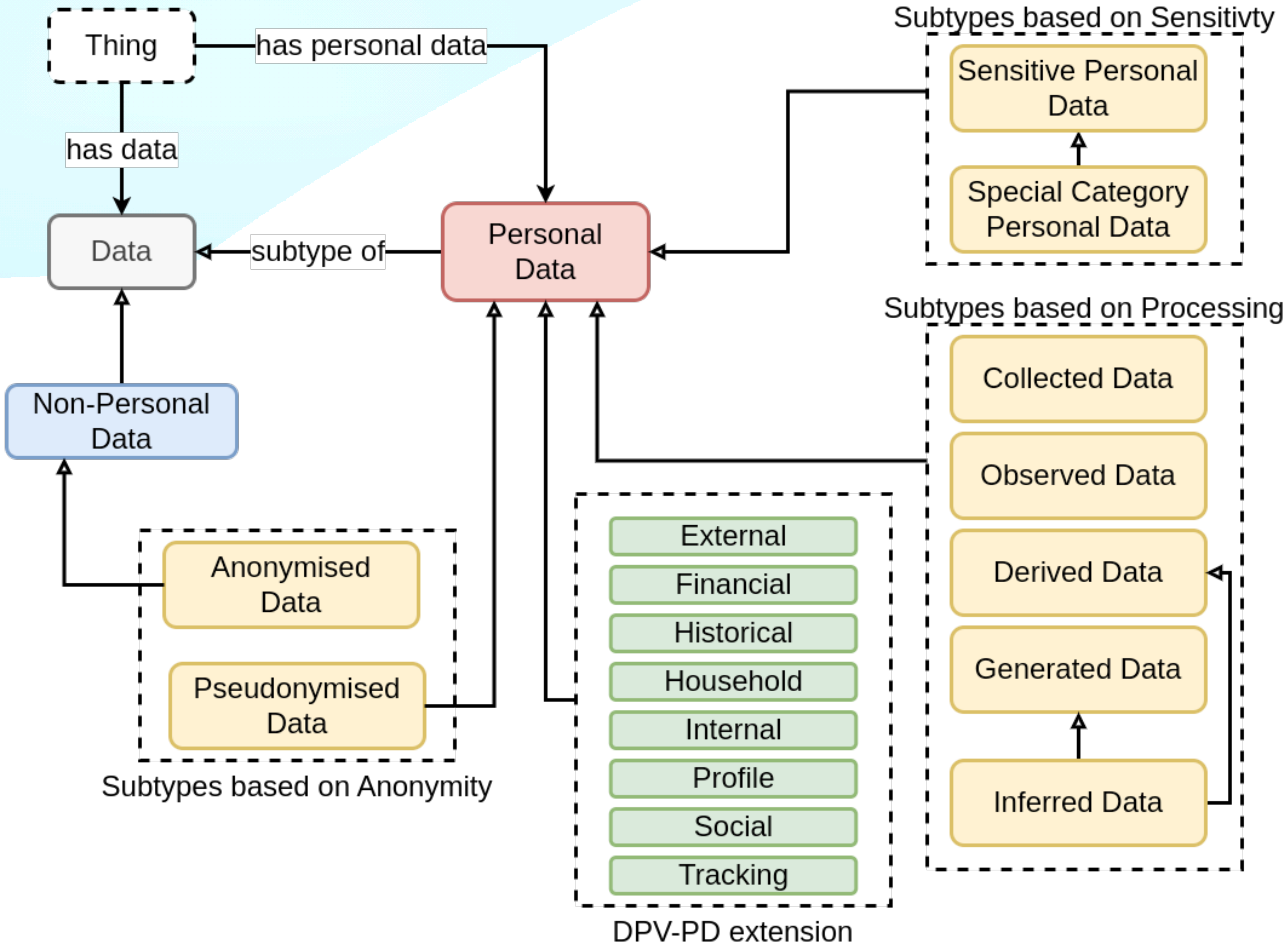
ISO 29100:2011

“Personal information” means information that **identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly**, with a particular consumer or household.

CCPA 1798.140 (o)(1)

Data

Personal Data



Personal Data

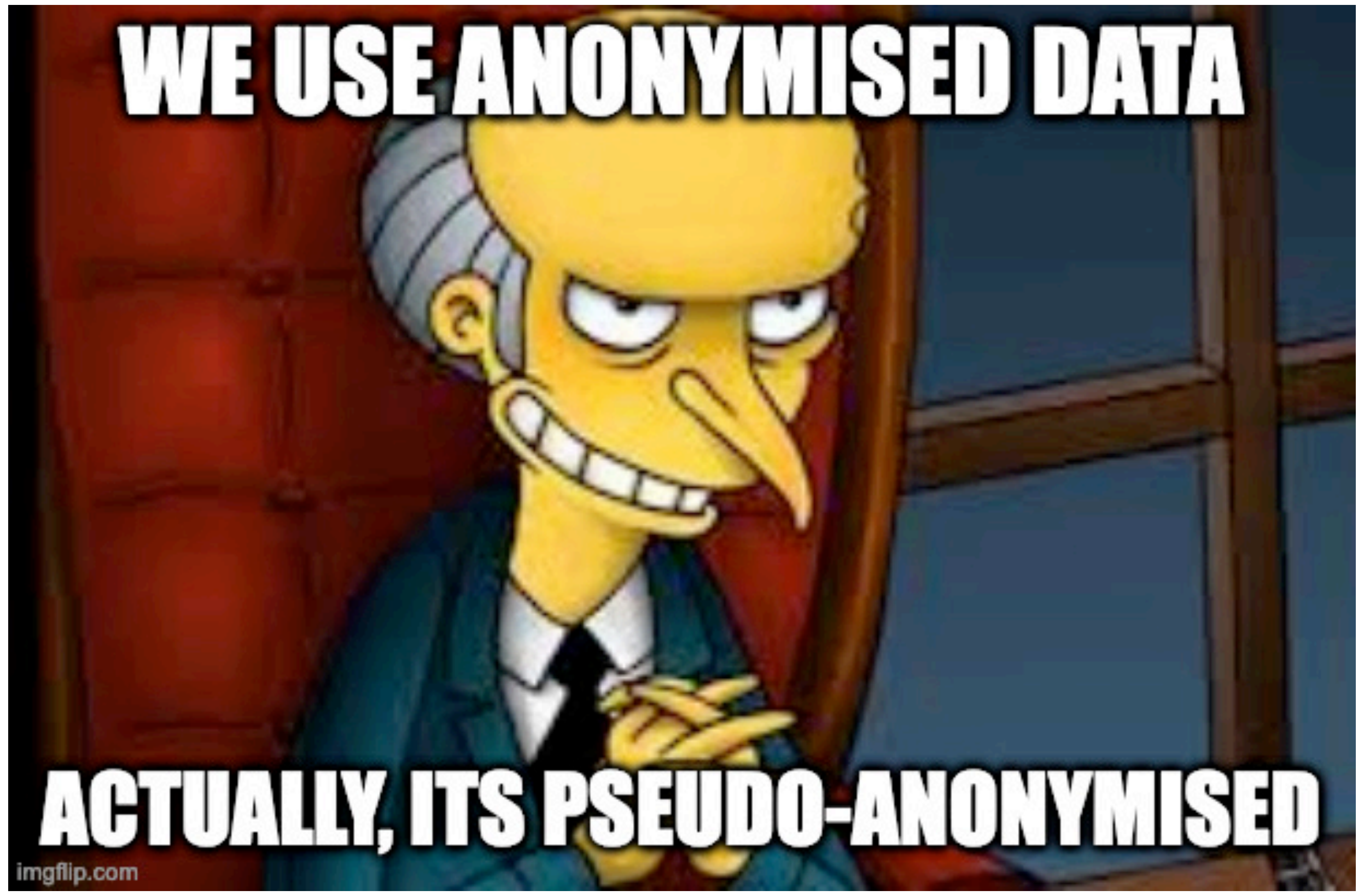
Identifiers, and Identifiability

1. Identifiers: Harsh (name), xyz@email.com (email)
2. Non-identifiers: Black (hair), Brown (eyes), 1.66m (height), etc.
3. For a room full of people, combine non-identifier to uniquely identify a person (me) — thus creating an identifier !!!
4. Useful technique for **fingerprinting**, **profiling**, **tracking**

Q: When is Personal Data not 'Personal' anymore?

Ans: When it is (completely) anonymised

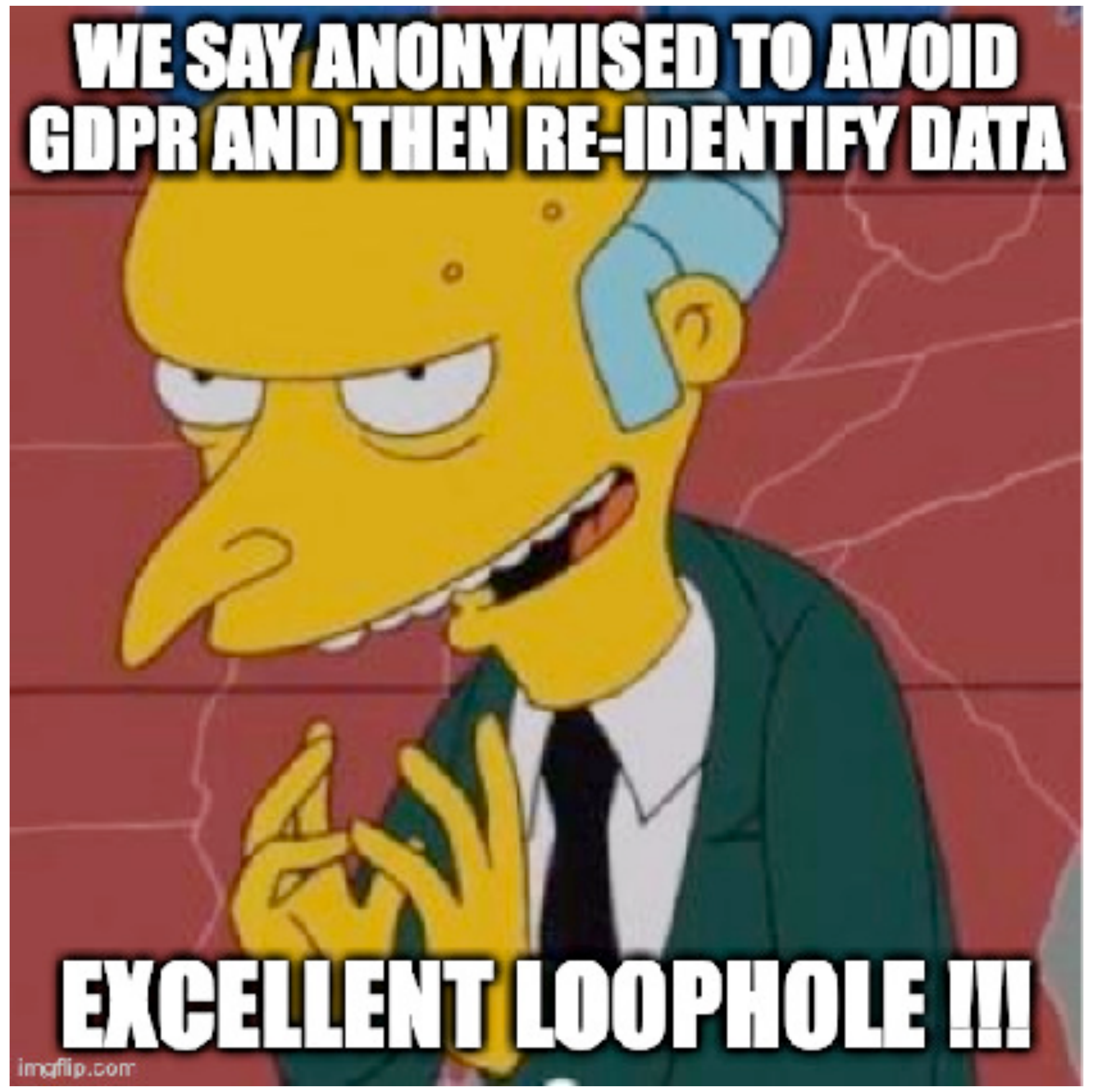
- Anonymisation is the removal of (some) 'identifying' attributes from data
- Merely using "**anonymisation**" does not produce anonymised data
- It produces '**pseudo-anonmised**' data, which is still personal data
- 'Completely anonymised' if it is **not identifiable**
- E.g.
  - Your exact location = personal data
  - approx. house = still personal data
  - approx. area = still personal data, but less
  - City = still personal data, but lesser
  - Country = anonymised, kind of

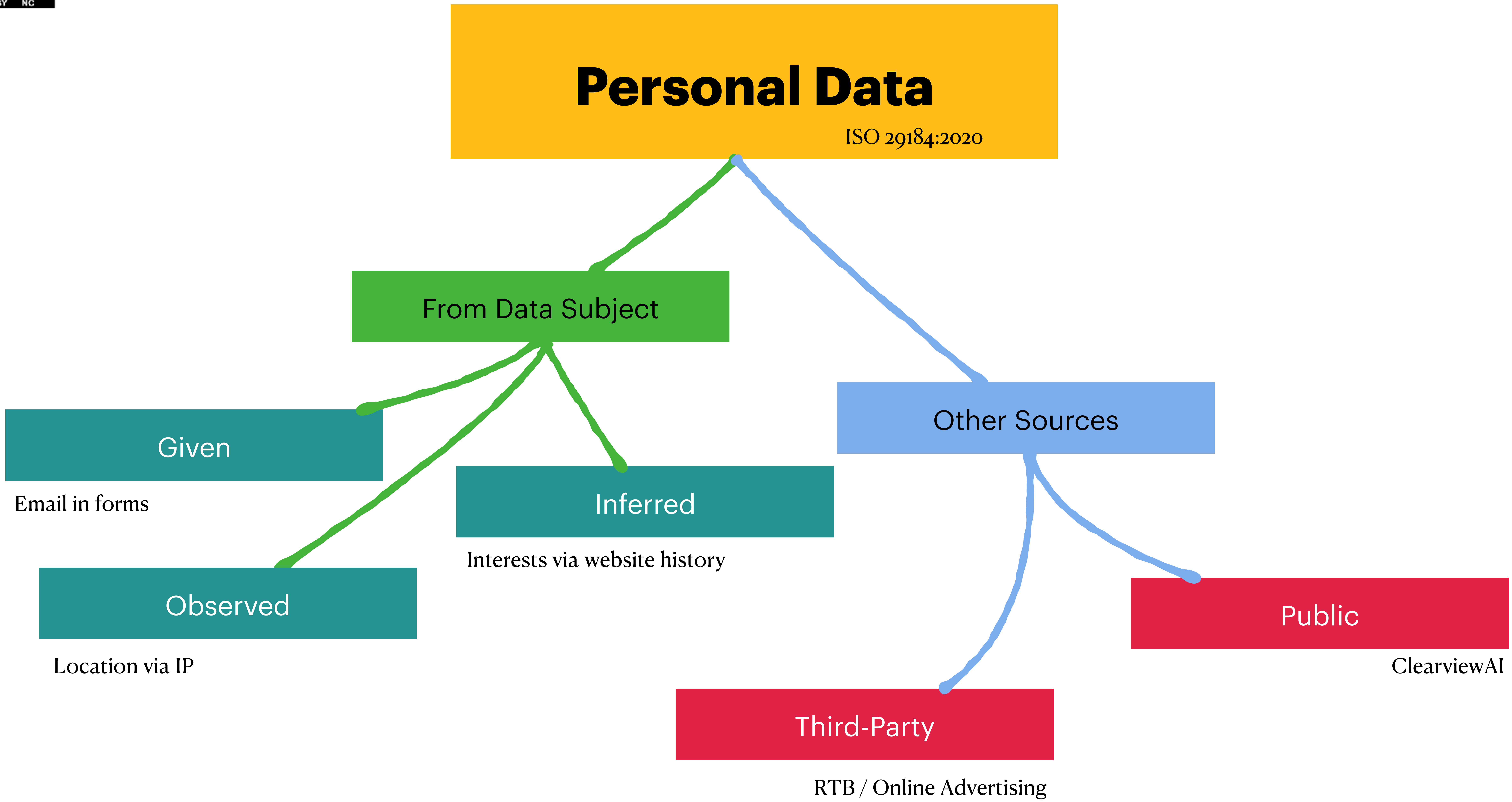


Q: When is Anonymised Data not Anonymised?

Ans: When it is possible to 're-identify' using any (practical) means possible

- Data is anonymised, i.e. all identifiers like names and emails are removed
- But using a 'combination' of remaining data points, a person is still identified
- Since **re-identification** is possible, its not '**fully anonymised**'
- 'Exploits'
  - Aggregated location — person's routines are unique
  - Voting and voters data
  - Fingerprinting - browser configurations, preferences
- GDPR applies to all the above since it is 'personal data'





Personal Data

ISO 29184:2020

From Data Subject

Given

Email in forms

Observed

Location via IP

Inferred

Interests via website history

Other Sources

Third-Party

RTB / Online Advertising

Public

ClearviewAI

Personal Data: Sensitive, and Special

Special category personal data is to GDPR what Ferrero Rocher is to chocolates

Sensitive:

- data that merits additional security

- older term used widely

Special:

- requires additional/specific legal permissions

- newer term introduced in GDPR

GDPR Prohibits

Processing of Special Categories of Personal Data

and

Requires additional obligations via legal basis in Article. 9

racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited

Processing

GDPR

GDPR Article 4(11)

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Notable alignment with ‘common’ terms used in documents, interfaces, etc.

collect, store, use, share, delete

Systematic Monitoring

Evaluation & Scoring

Matching & Combining

Automated Decision Making

Innovative Use of New Technologies

GDPR Article.35 Data Protection Impact Assessments

GDPR applies before Processing starts

Common Misinterpretations

- Data collected but 'anonymised' is not subject to GDPR
- If data isn't shared, nothing needs to be declared
- Collecting anonymised data and attaching an identifier to it
- Hiding things that require transparency and permission
    - Scale and scope of processing
    - Involvement of special categories
    - Involvement of any automated decision making
    - Creating, sharing, using - profiling

LOOK, I'VE FOUND SOME DATA
LETS SAY I 'ANONYMISE' IT AFTER COLLECTION
imgflip.com

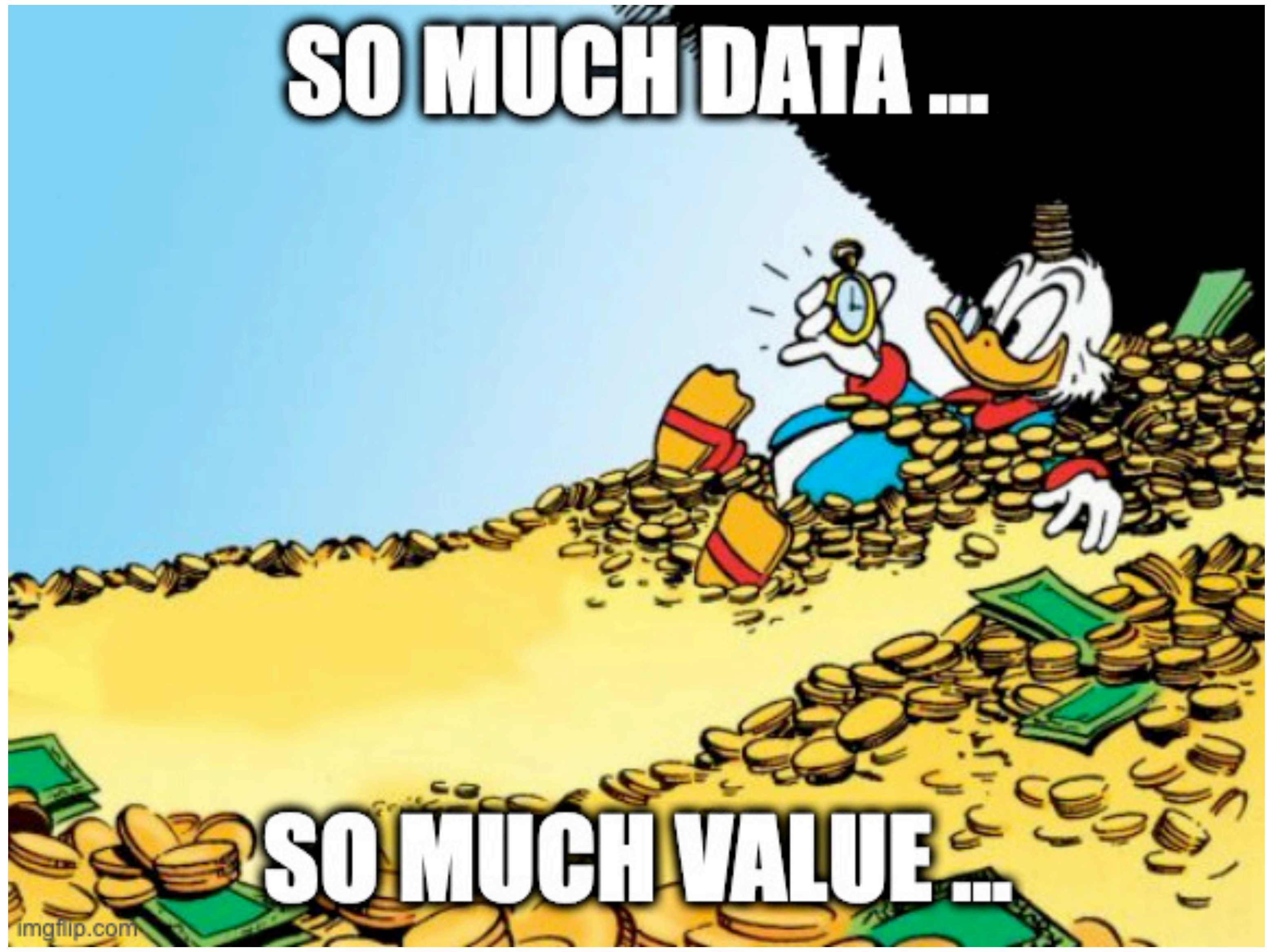
Purpose

GDPR

All Processing in GDPR *must* be towards a Goal

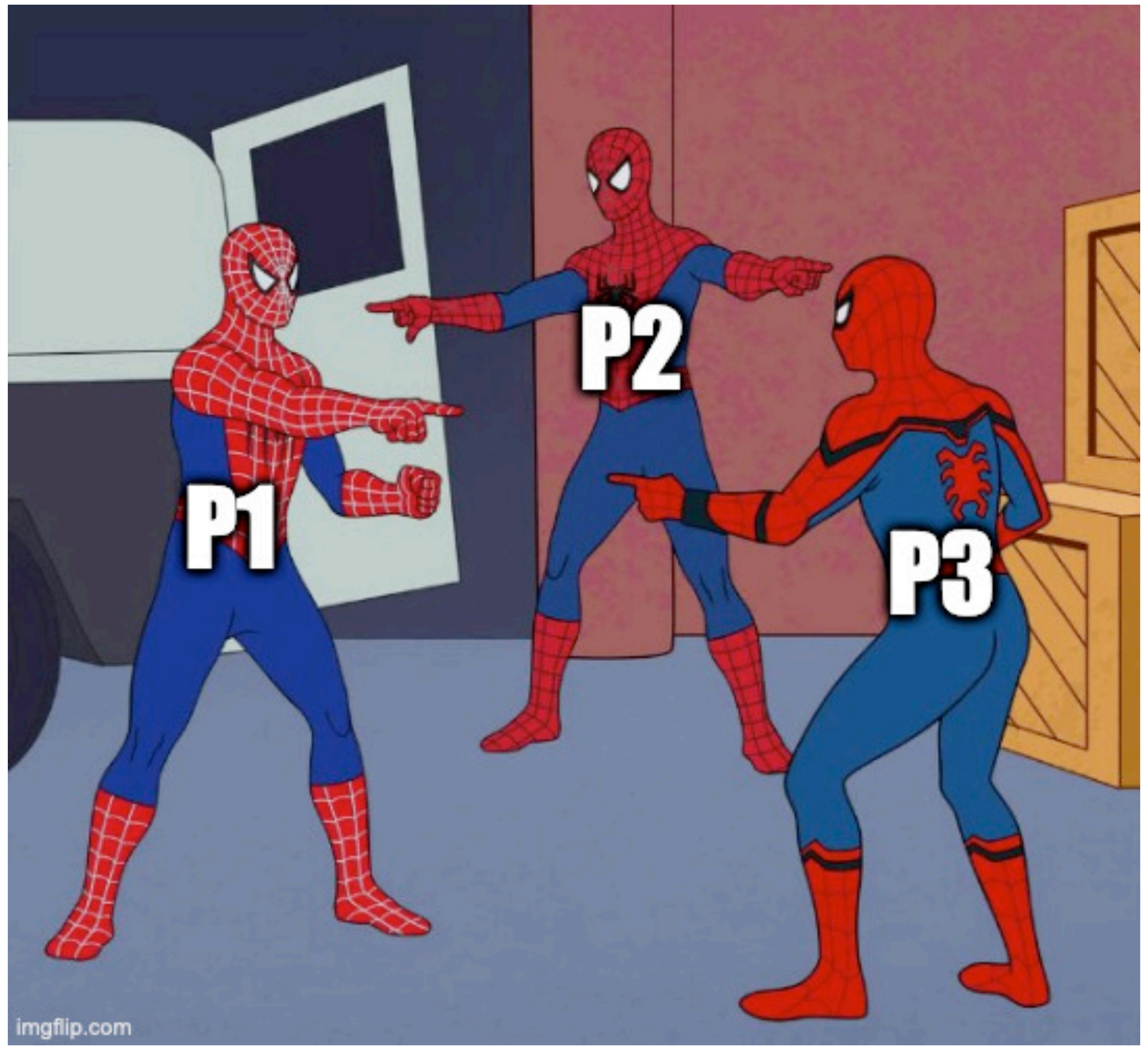
Implied when a 'Purpose' is necessary as per Article.5

Every Processing *must* have a Purpose



WE COLLECT DATA TO ENHANCE YOUR EXPERIENCE
THAT'S A BULLSHIT PURPOSE
WHY ... ?
imgflip.com

Purposes must be separate from other matter, including other purposes



Purposes must be *specific* and *unambiguous*

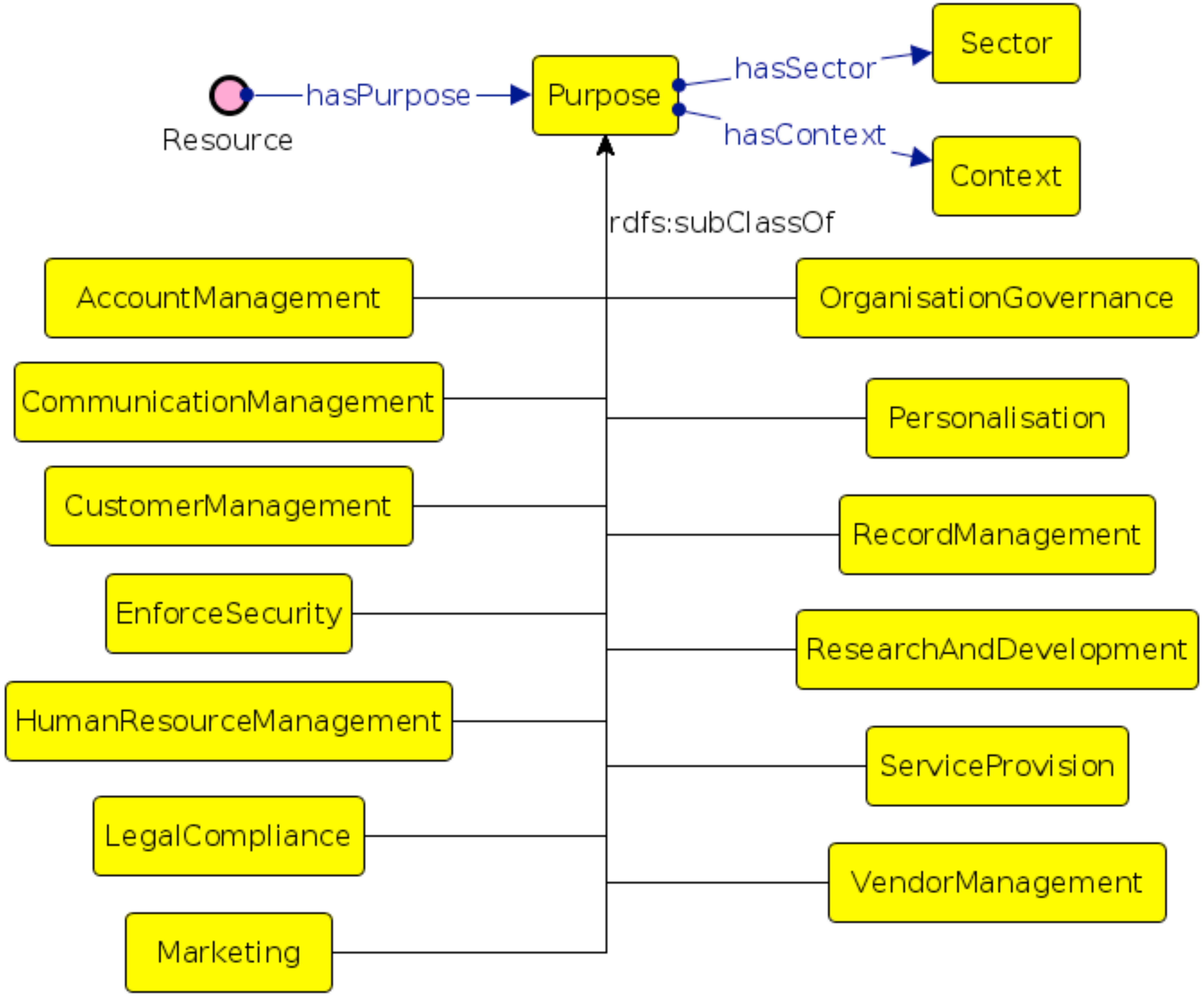
Purposes are intended to be human-readable and human-comprehensible

Purposes should not be broad and abstract

Purposes should be specific and contextual to their use-case

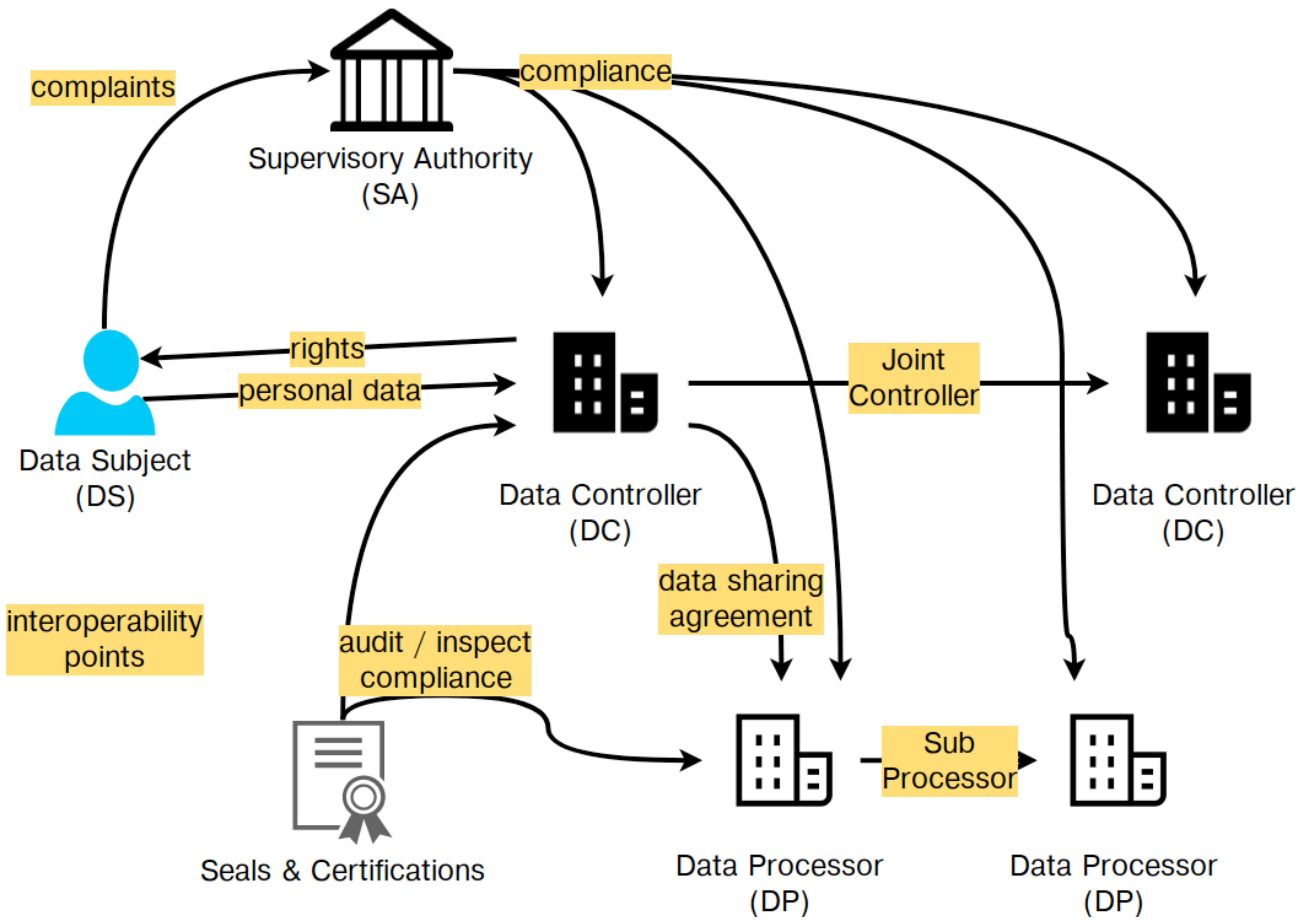
Purposes can be grouped or categorised, but not replaced, e.g. with Marketing for 'Sending new product emails'

Purposes don't have to necessarily benefit the data subject e.g. service optimisation



Actors

GDPR



Data Controllers are responsible for deciding the 'purpose'

Data Controllers may not even 'touch' the data they 'control'

Data Controllers can 'team up' to become Joint (Data) Controllers

Processors only act on 'orders' given (explicitly) by Controllers

Processors can appoint other (sub-)Processors, still governed by instructions from Controllers

Processors deciding/ processing on their own become Controllers

Data Protection Authorities (DPA) are empowered by GDPR to enforce its obligations on all entities

GDPR Data Interoperability Model,
EURAS Annual Standardisation Conference (EURAS) 2018,
Harshvardhan J. Pandit* , Declan O'Sullivan , Dave Lewis
https://harshp.com/research/publications/010-gdpr-data-interoperability-model

Legal Basis & Principles

GDPR

GDPR’s Framework of Legal Basis

A.6(1-b)
Contract

A.6(1-c)
Legal Obligation

A.6(1-e)
Public Interest

A.6(1-d)
Protect vital interests of data subject or other natural person

A.6(1-c)
Official Authority of Controller

A.6(1-a)
Consent

A.6(1-f)
Legitimate Interest of Controller

A.6(1-f)
Legitimate Interest of Third-Party

Widespread Problematic Occurrences

GDPR's principles providing a framework for ‘responsibility'

Principles (Article.5)

lawfulness, fairness and transparency
purpose limitation
data minimisation
accuracy
storage limitation
integrity and confidentiality
accountability

Consent (Article.7)

Informed
Freely Given
Unambiguous
Balance of Power(s)
Right to Withdraw
Explicit Consent (e.g. for Article.9)

A12-A22 Rights

Transparency (A.12)
Notice (A.13, A.14) ;
Object to Processing
Rectification of Data
Erasure (Right to be Forgotten)
Restriction of Processing
Right of Access
Data Portability

A77 **Right to complaint**

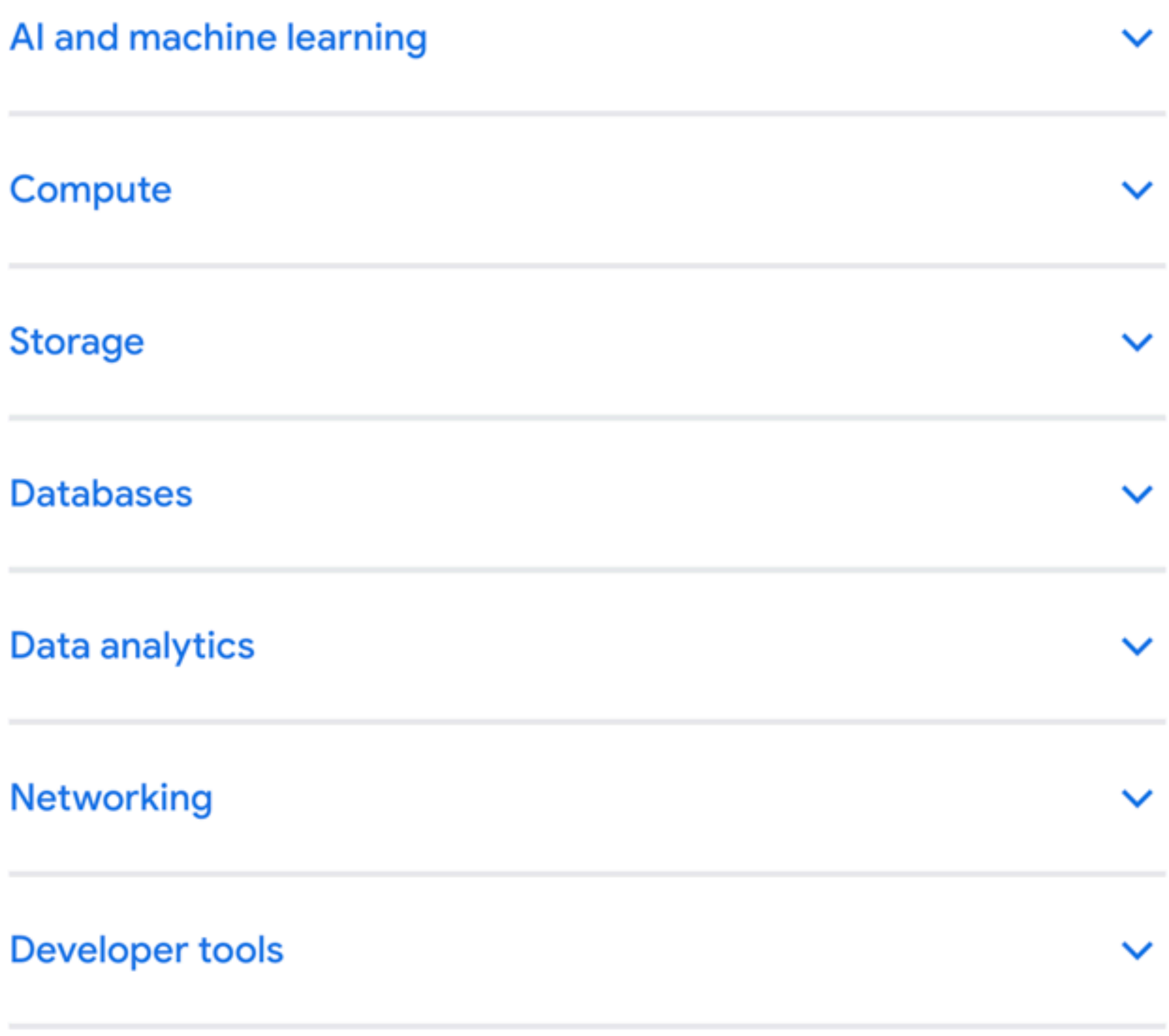
Any Data Subject can complaint to their Supervisory Authority (DPA)
If DPA is in a different country than the company, then the DPA will ‘lease’ and ‘co-operate’ with the DPA of that country

Cloud

GDPR

What are you doing with the “Personal Data”?

Cloud can be used to collect, store, use, share, delete data



- AI and machine learning
- Compute
- Storage
- Databases
- Data analytics
- Networking
- Developer tools

https://cloud.google.com/?hl=en

DCU

aws

ADAPT

Azure

Google Cloud

Cloud Security

Biggest Risks

https://www.dataprotection.ie/en/dpc-guidance/five-steps-secure-cloud-based-environments

Cloud-based environments offer many advantages to organisations. However, they also introduce a number of technical security risks which organisations should be aware of such as:

—> Data breaches

—> Hijacking of accounts

—> Unauthorised access to personal data

Cloud Security

Measures

https://www.dataprotection.ie/en/dpc-guidance/five-steps-secure-cloud-based-environments

Organisations should apply such technical security and organisational security measures in a layered manner consisting of but not limited to:

—> Access controls

—> Firewalls

—> Antivirus

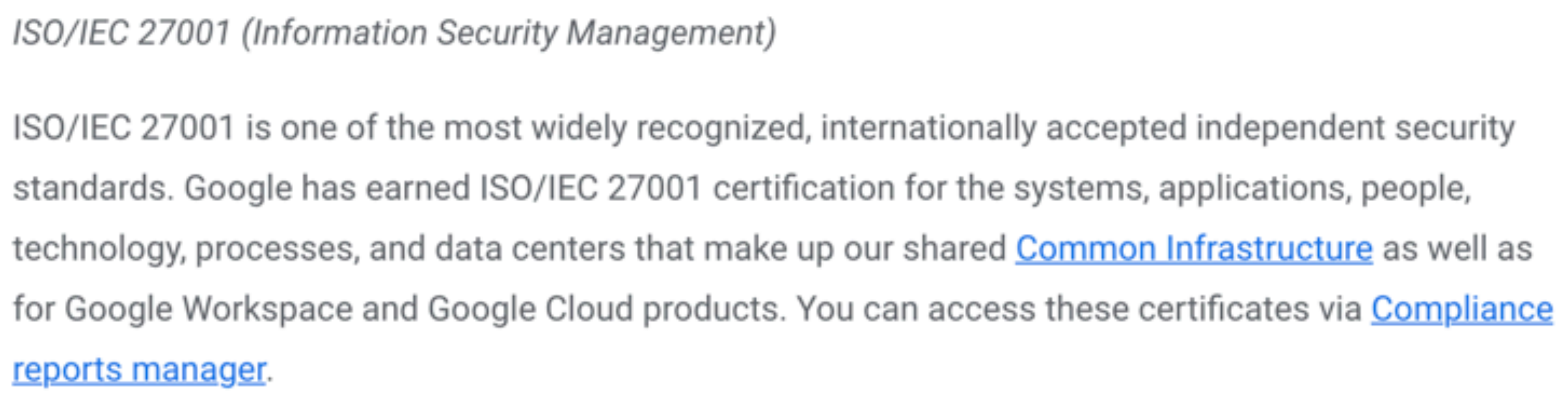
—> **Staff training**

—> **Policy development**

A layered approach to cloud-based security mitigates the risk of a single security measure failing which may result in a personal data breach.

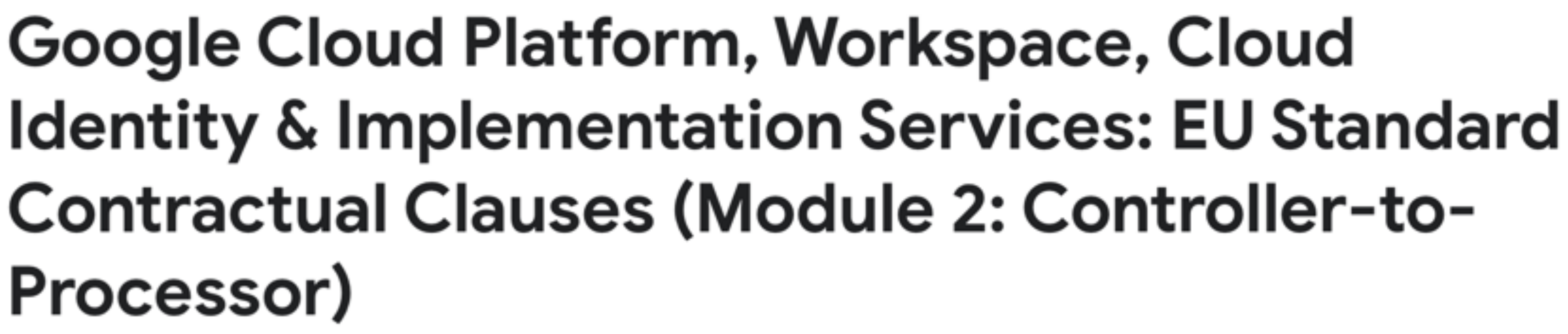
https://www.dataprotection.ie/en/dpc-guidance/five-steps-secure-cloud-based-environments

Choose a Cloud service provider that incorporates GDPR or has the specific measures you are looking for

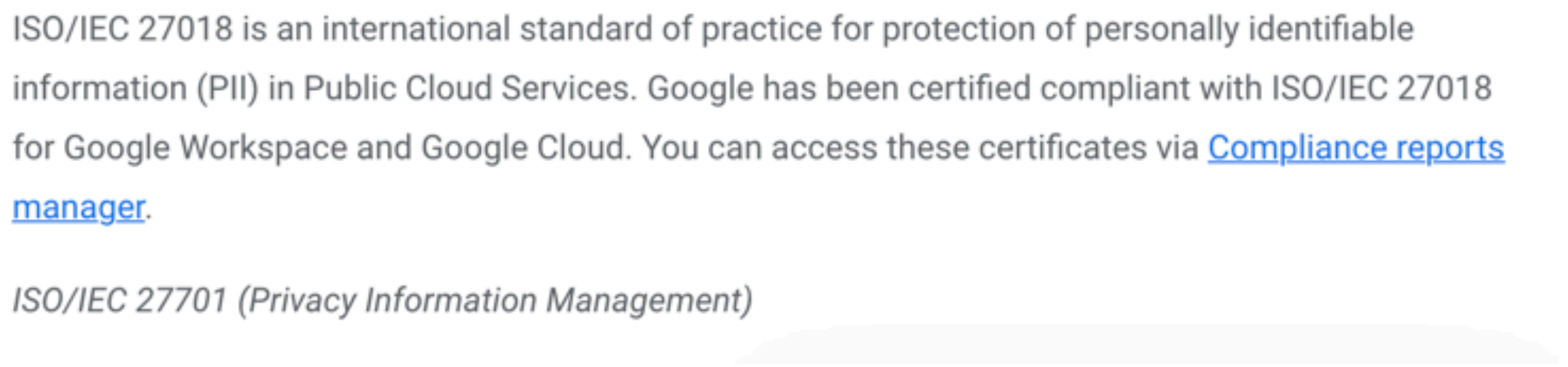


ISO/IEC 27001 (Information Security Management)

ISO/IEC 27001 is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO/IEC 27001 certification for the systems, applications, people, technology, processes, and data centers that make up our shared Common Infrastructure as well as for Google Workspace and Google Cloud products. You can access these certificates via Compliance reports manager.

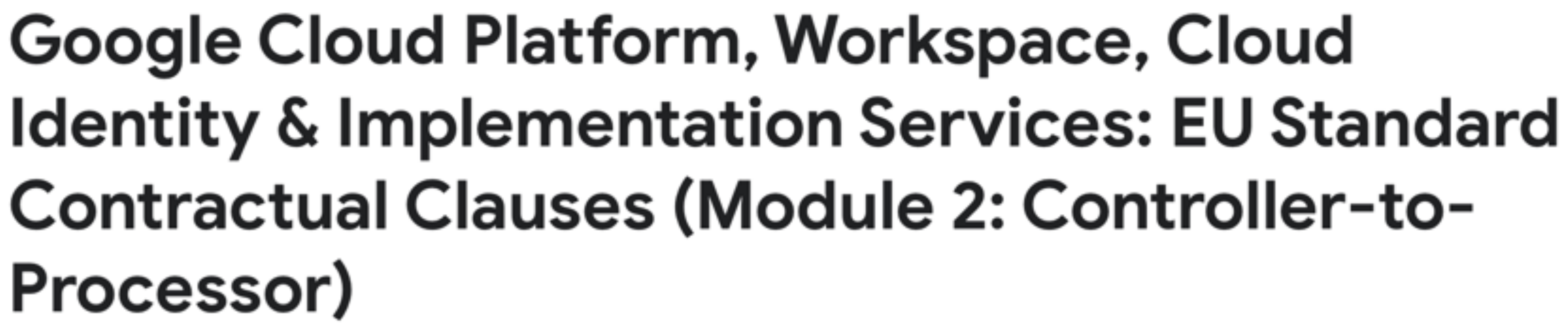


Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 2: Controller-to-Processor)

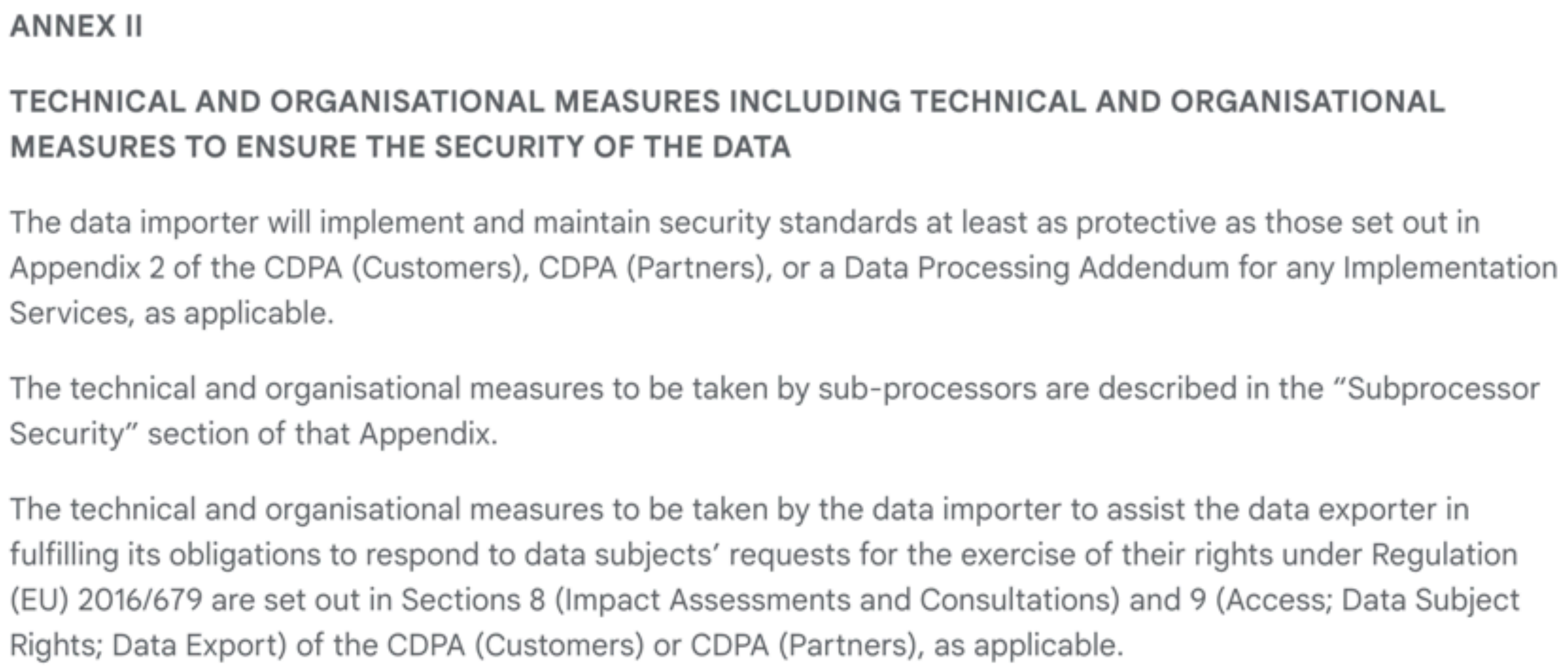


ISO/IEC 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO/IEC 27018 for Google Workspace and Google Cloud. You can access these certificates via Compliance reports manager.

ISO/IEC 27701 (Privacy Information Management)



Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 2: Controller-to-Processor)



ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer will implement and maintain security standards at least as protective as those set out in Appendix 2 of the CDPA (Customers), CDPA (Partners), or a Data Processing Addendum for any Implementation Services, as applicable.

The technical and organisational measures to be taken by sub-processors are described in the "Subprocessor Security" section of that Appendix.

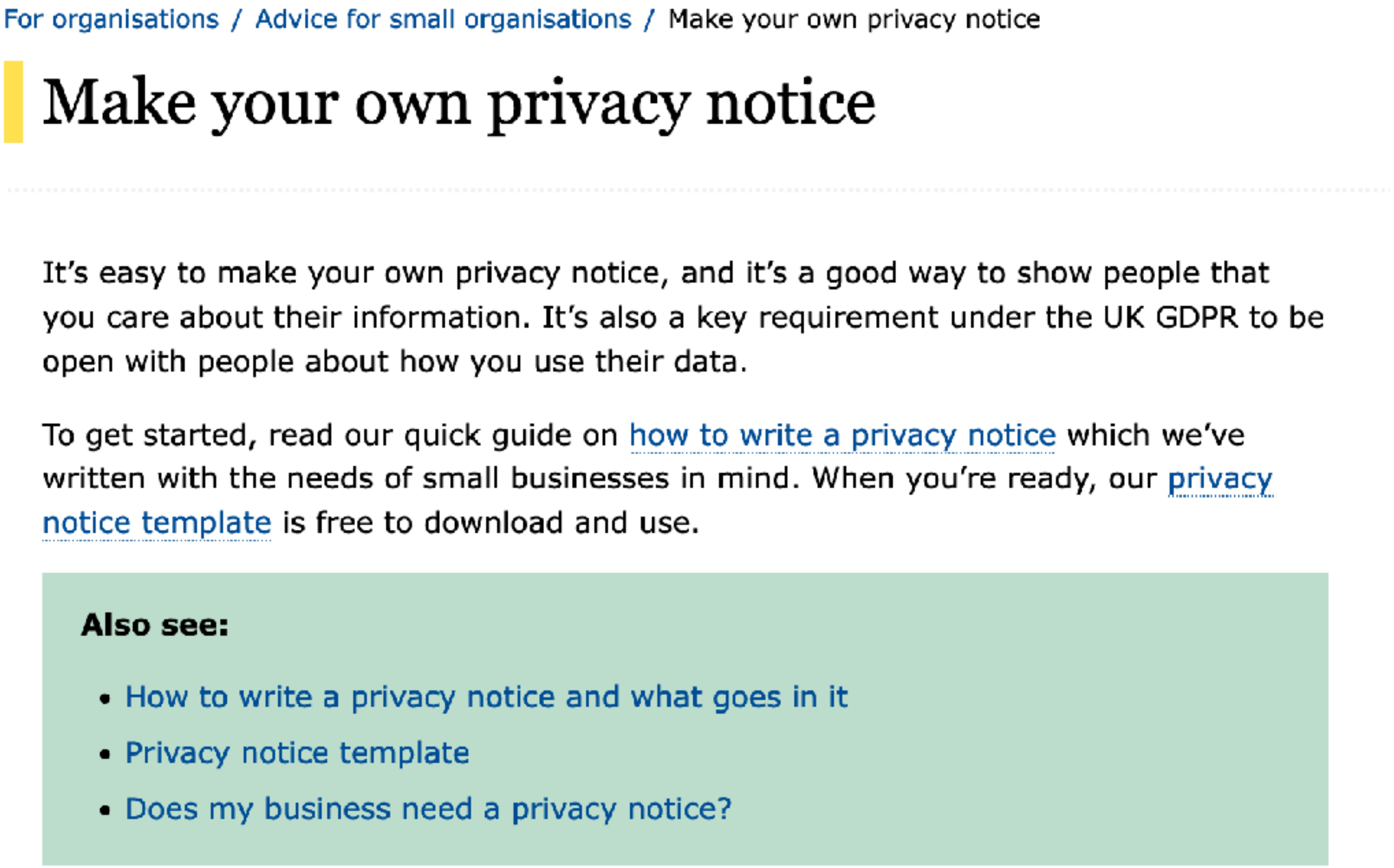
The technical and organisational measures to be taken by the data importer to assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 are set out in Sections 8 (Impact Assessments and Consultations) and 9 (Access; Data Subject Rights; Data Export) of the CDPA (Customers) or CDPA (Partners), as applicable.

https://cloud.google.com/terms/sccs/eu-c2p

Privacy Notices

Also called a *Privacy Policy*

https://www.dataprotection.ie/en/dpc-guidance/five-steps-secure-cloud-based-environments



For organisations / Advice for small organisations / Make your own privacy notice

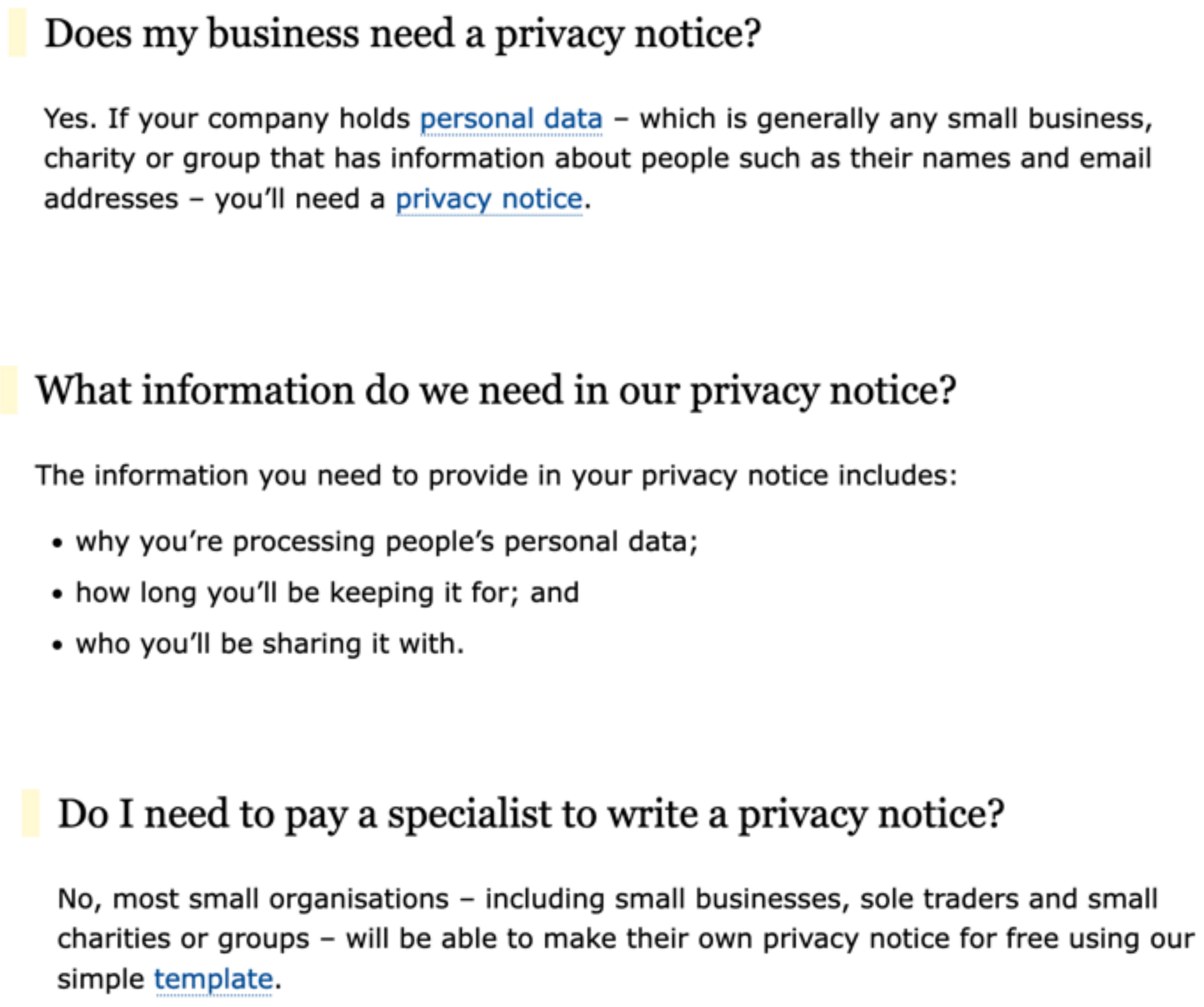
Make your own privacy notice

It's easy to make your own privacy notice, and it's a good way to show people that you care about their information. It's also a key requirement under the UK GDPR to be open with people about how you use their data.

To get started, read our quick guide on how to write a privacy notice which we've written with the needs of small businesses in mind. When you're ready, our privacy notice template is free to download and use.

Also see:

- How to write a privacy notice and what goes in it
- Privacy notice template
- Does my business need a privacy notice?



Does my business need a privacy notice?

Yes. If your company holds personal data – which is generally any small business, charity or group that has information about people such as their names and email addresses – you'll need a privacy notice.

What information do we need in our privacy notice?

The information you need to provide in your privacy notice includes:

- why you're processing people's personal data;
- how long you'll be keeping it for; and
- who you'll be sharing it with.

Do I need to pay a specialist to write a privacy notice?

No, most small organisations – including small businesses, sole traders and small charities or groups – will be able to make their own privacy notice for free using our simple template.

https://ico.org.uk/for-organisations/advice-for-small-organisations/make-your-own-privacy-notice/

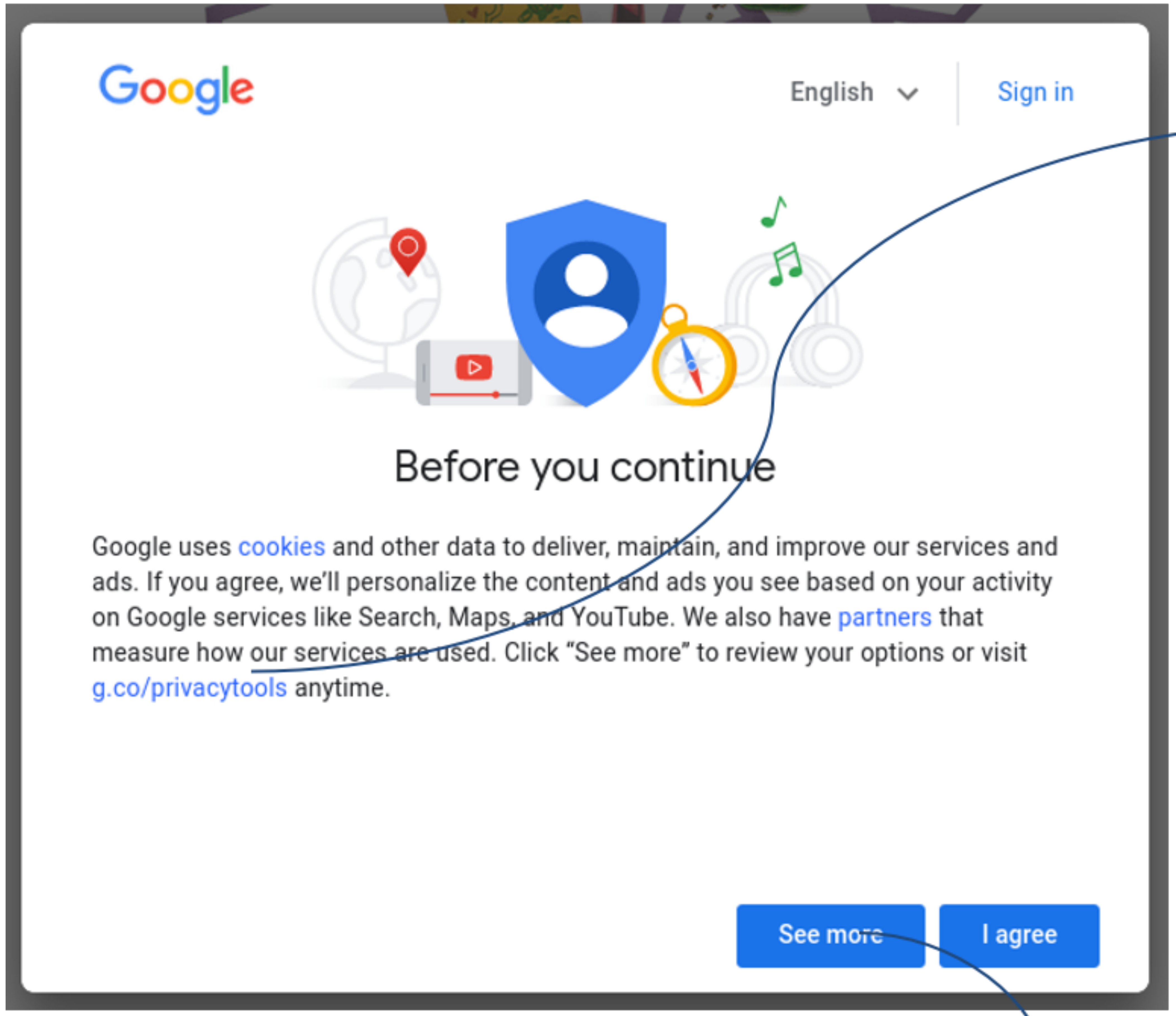
Consent

GDPR

Ever visited a website and got blocked by a popup?

Was it annoying?
Why was it there?
What do you think is the quickest way to get rid of it?

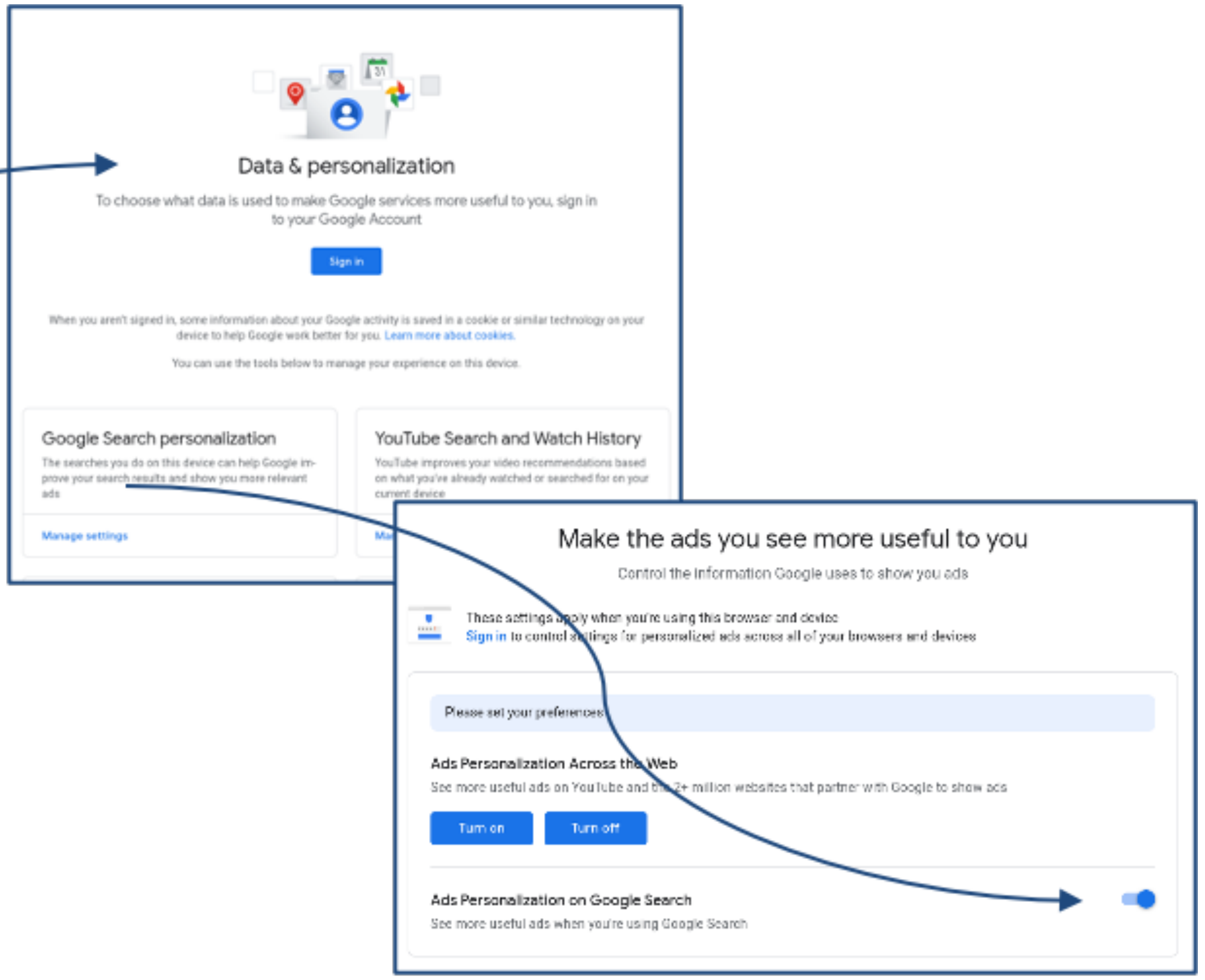
WE SHARE YOUR PHOTOS WITH OUR PARTNERS TO FIND THE FAIREST OF THEM ALL
ACCEPT ALL
MORE SETTINGS
imgflip.com



Before you continue

Google uses cookies and other data to deliver, maintain, and improve our services and ads. If you agree, we'll personalize the content and ads you see based on your activity on Google services like Search, Maps, and YouTube. We also have partners that measure how our services are used. Click "See more" to review your options or visit g.co/privacytools anytime.

Consent dialogue on https://google.ie MAR-14 2021



Data & personalization

To choose what data is used to make Google services more useful to you, sign in to your Google Account

When you aren't signed in, some information about your Google activity is saved in a cookie or similar technology on your device to help Google work better for you. Learn more about cookies.

You can use the tools below to manage your experience on this device.

Google Search personalization

The searches you do on this device can help Google improve your search results and show you more relevant ads

YouTube Search and Watch History

YouTube improves your video recommendations based on what you've already watched or searched for on your current device

Make the ads you see more useful to you

Control the information Google uses to show you ads

These settings apply when you're using this browser and device
Sign in to control settings for personalized ads across all of your browsers and devices

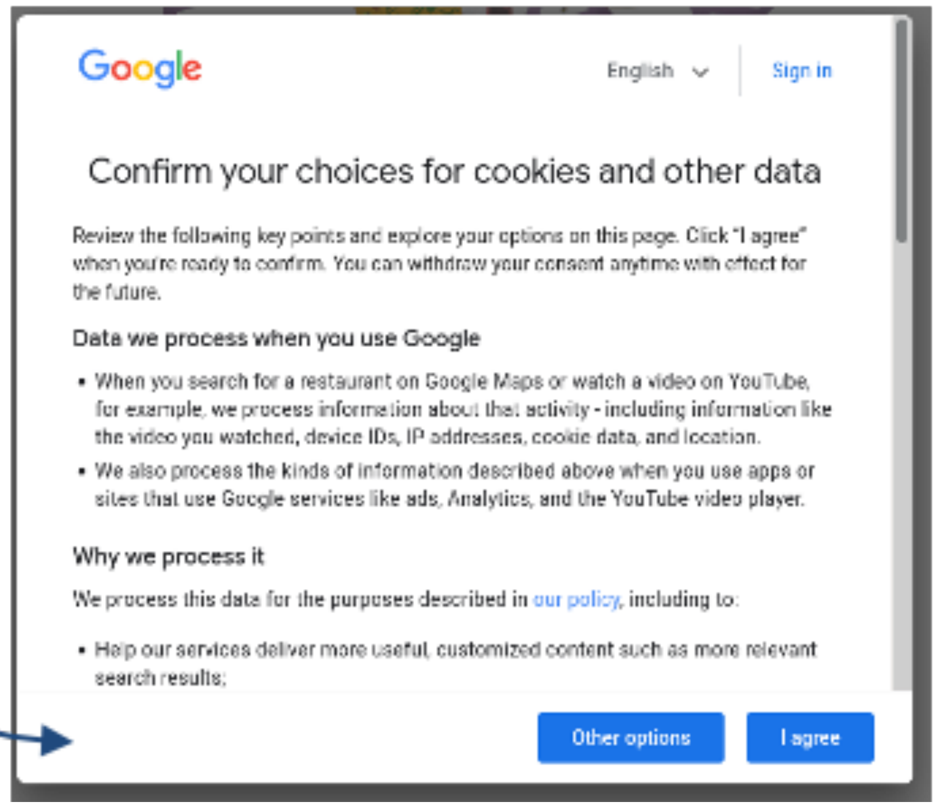
Please set your preferences

Ads Personalization Across the Web

See more useful ads on YouTube and the 2+ million websites that partner with Google to show ads

Ads Personalization on Google Search

See more useful ads when you're using Google Search



Confirm your choices for cookies and other data

Review the following key points and explore your options on this page. Click "I agree" when you're ready to confirm. You can withdraw your consent anytime with effect for the future.

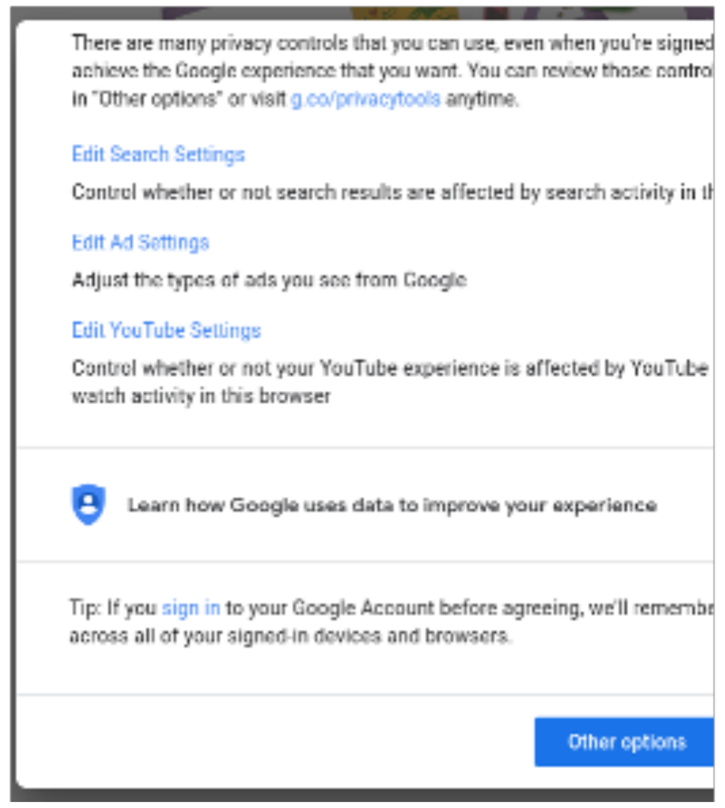
Data we process when you use Google

- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity - including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it

We process this data for the purposes described in our policy, including to:

- Help our services deliver more useful, customized content such as more relevant search results;



There are many privacy controls that you can use, even when you're signed achieve the Google experience that you want. You can review those contro in "Other options" or visit g.co/privacytools anytime.

Edit Search Settings

Control whether or not search results are affected by search activity in th

Edit Ad Settings

Adjust the types of ads you see from Google

Edit YouTube Settings

Control whether or not your YouTube experience is affected by YouTube watch activity in this browser

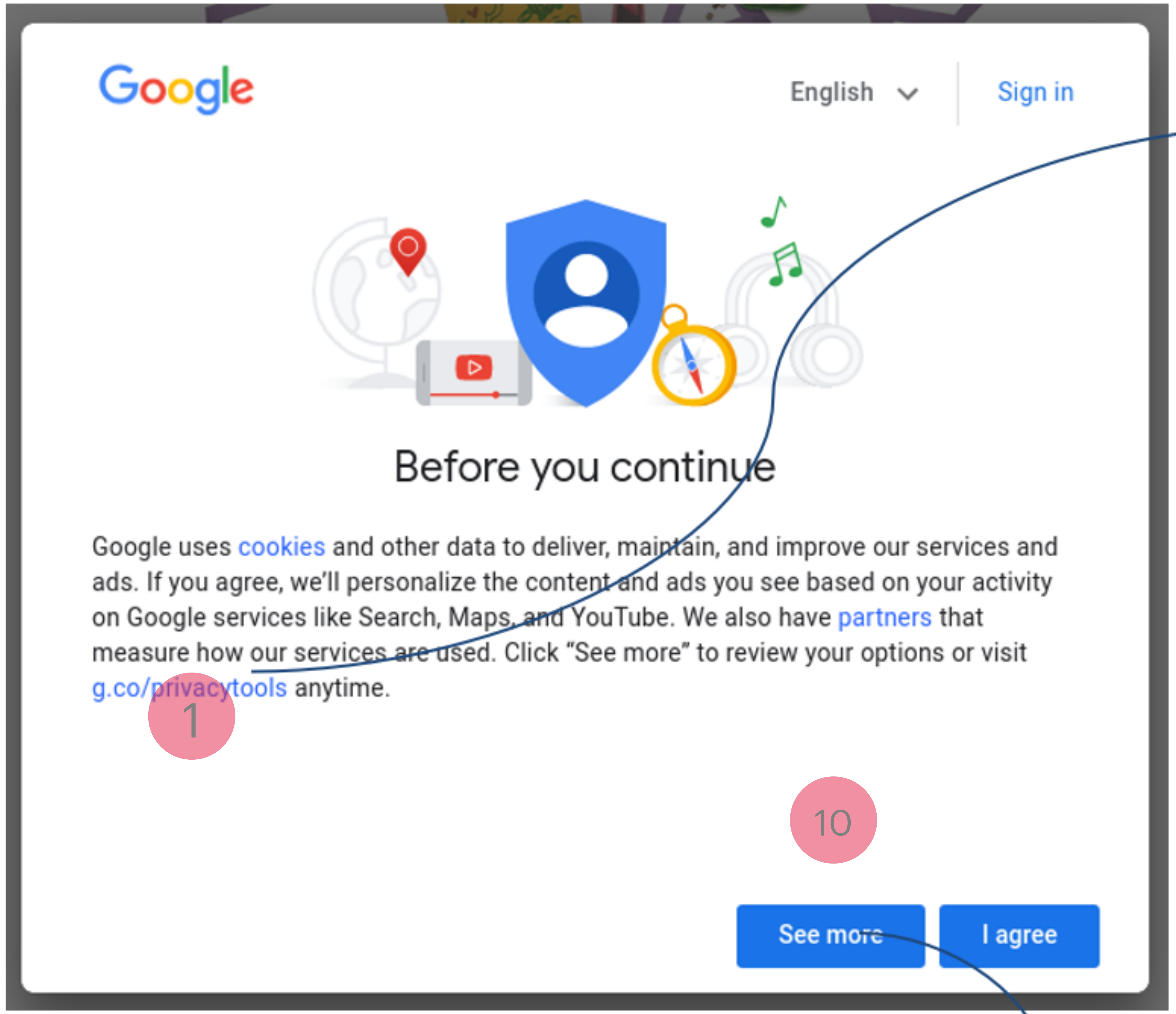
Learn how Google uses data to improve your experience

Tip: If you sign in to your Google Account before agreeing, we'll rememb across all of your signed-in devices and browsers.

Companies are required to show you a "NOTICE" informing what data they collect and how they use it.

Where this is based on your CONSENT, they need to ask your permission before they can proceed.

Since every website visit collects and uses your personal data, this means there's a notice & consent process every time you visit a website ...



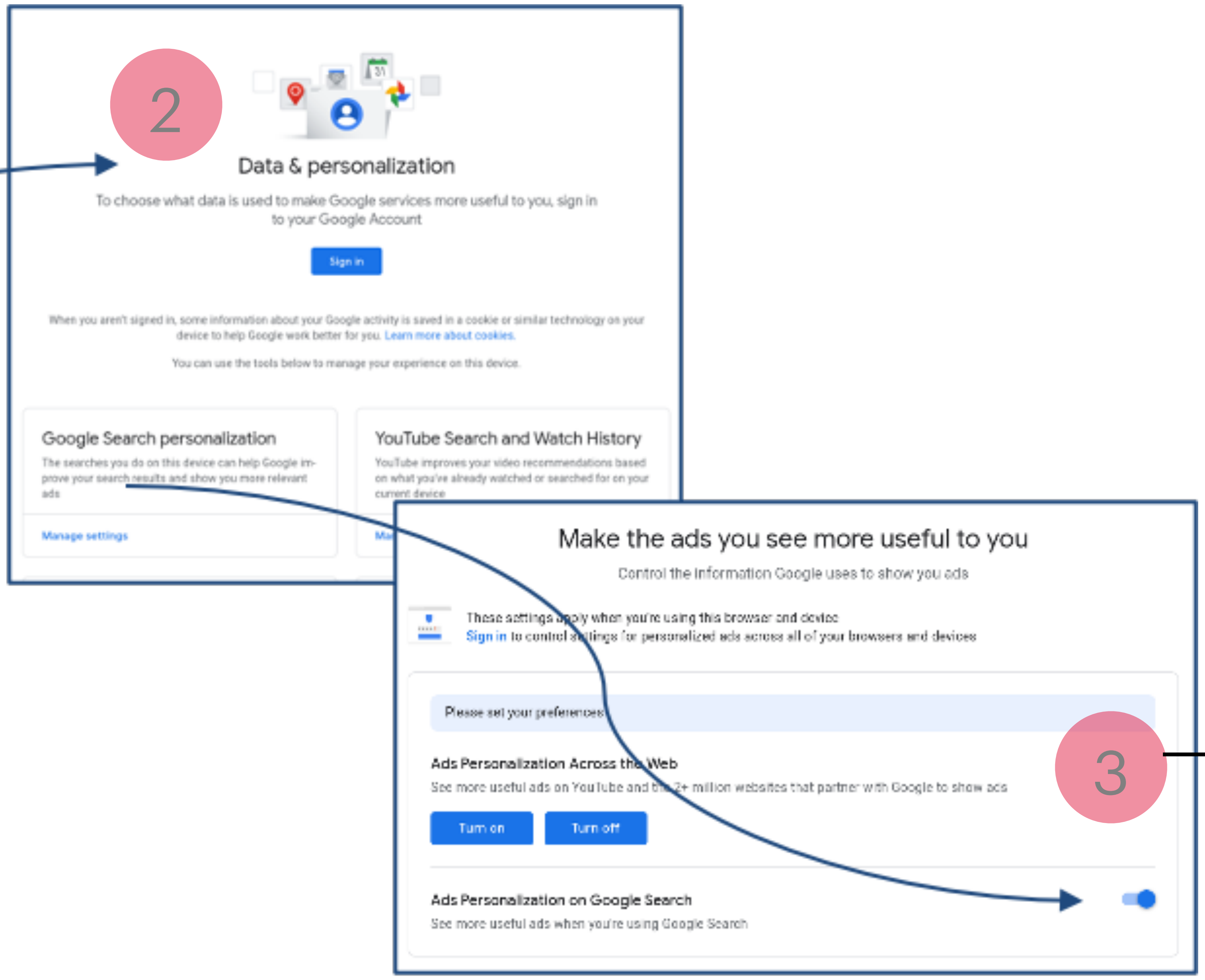
Google English Sign in

Before you continue

Google uses cookies and other data to deliver, maintain, and improve our services and ads. If you agree, we'll personalize the content and ads you see based on your activity on Google services like Search, Maps, and YouTube. We also have partners that measure how our services are used. Click "See more" to review your options or visit g.co/privacytools anytime.

See more | I agree

Consent dialogue on https://google.ie MAR-14 2021



Data & personalization

To choose what data is used to make Google services more useful to you, sign in to your Google Account

Sign in

When you aren't signed in, some information about your Google activity is saved in a cookie or similar technology on your device to help Google work better for you. Learn more about cookies.

You can use the tools below to manage your experience on this device.

Google Search personalization

The searches you do on this device can help Google improve your search results and show you more relevant ads

Manage settings

YouTube Search and Watch History

YouTube improves your video recommendations based on what you've already watched or searched for on your current device

Make the ads you see more useful to you

Control the information Google uses to show you ads

These settings apply when you're using this browser and device
Sign in to control settings for personalized ads across all of your browsers and devices

Please set your preferences

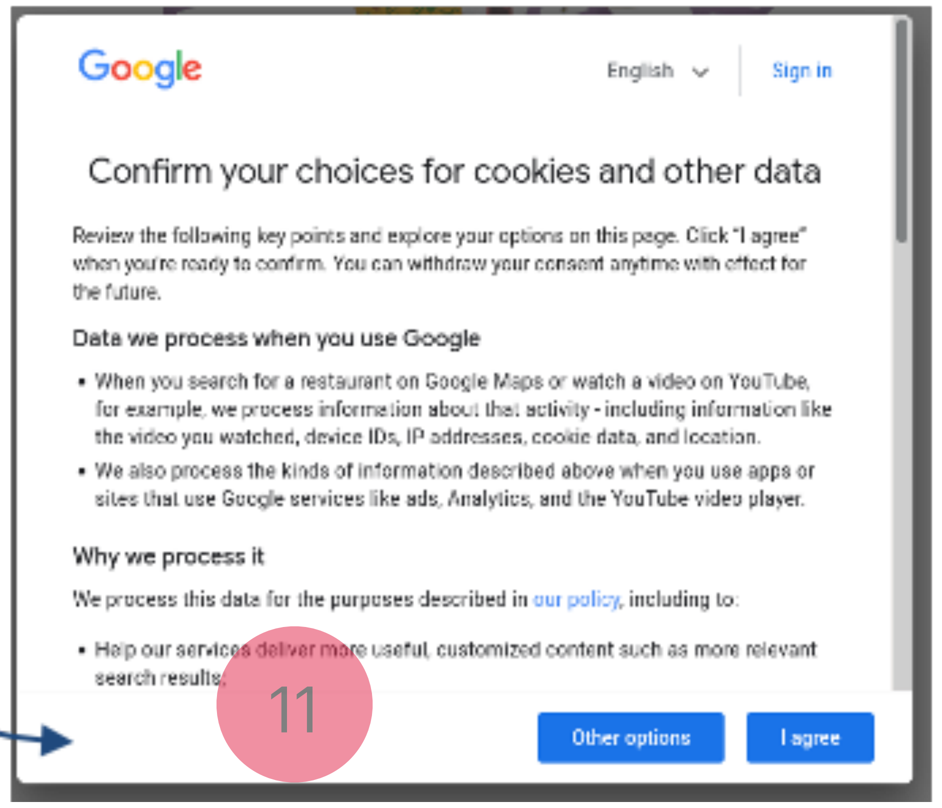
Ads Personalization Across the Web

See more useful ads on YouTube and the 2+ million websites that partner with Google to show ads

Turn on | Turn off

Ads Personalization on Google Search

See more useful ads when you're using Google Search



Google English Sign in

Confirm your choices for cookies and other data

Review the following key points and explore your options on this page. Click "I agree" when you're ready to confirm. You can withdraw your consent anytime with effect for the future.

Data we process when you use Google

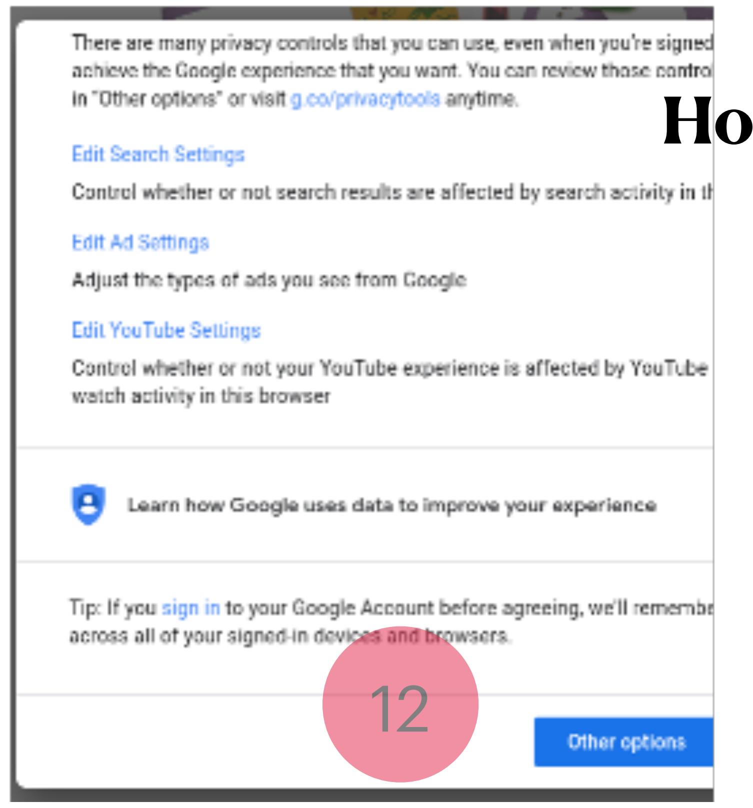
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity - including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it

We process this data for the purposes described in our policy, including to:

- Help our services deliver more useful, customized content such as more relevant search results;

Other options | I agree



There are many privacy controls that you can use, even when you're signed
achieve the Google experience that you want. You can review those contro
in "Other options" or visit g.co/privacytools anytime.

Edit Search Settings

Control whether or not search results are affected by search activity in th

Edit Ad Settings

Adjust the types of ads you see from Google

Edit YouTube Settings

Control whether or not your YouTube experience is affected by YouTube watch activity in this browser

Learn how Google uses data to improve your experience

Tip: If you sign in to your Google Account before agreeing, we'll rememb
across all of your signed-in devices and browsers.

Other options

Companies are required to show you a "NOTICE" informing what data they collect and how they use it.

Where this is based on your CONSENT, they need to ask your permission before they can proceed.

Since every website visit collects and uses your personal data, this means there's a notice & consent process every time you visit a website ...

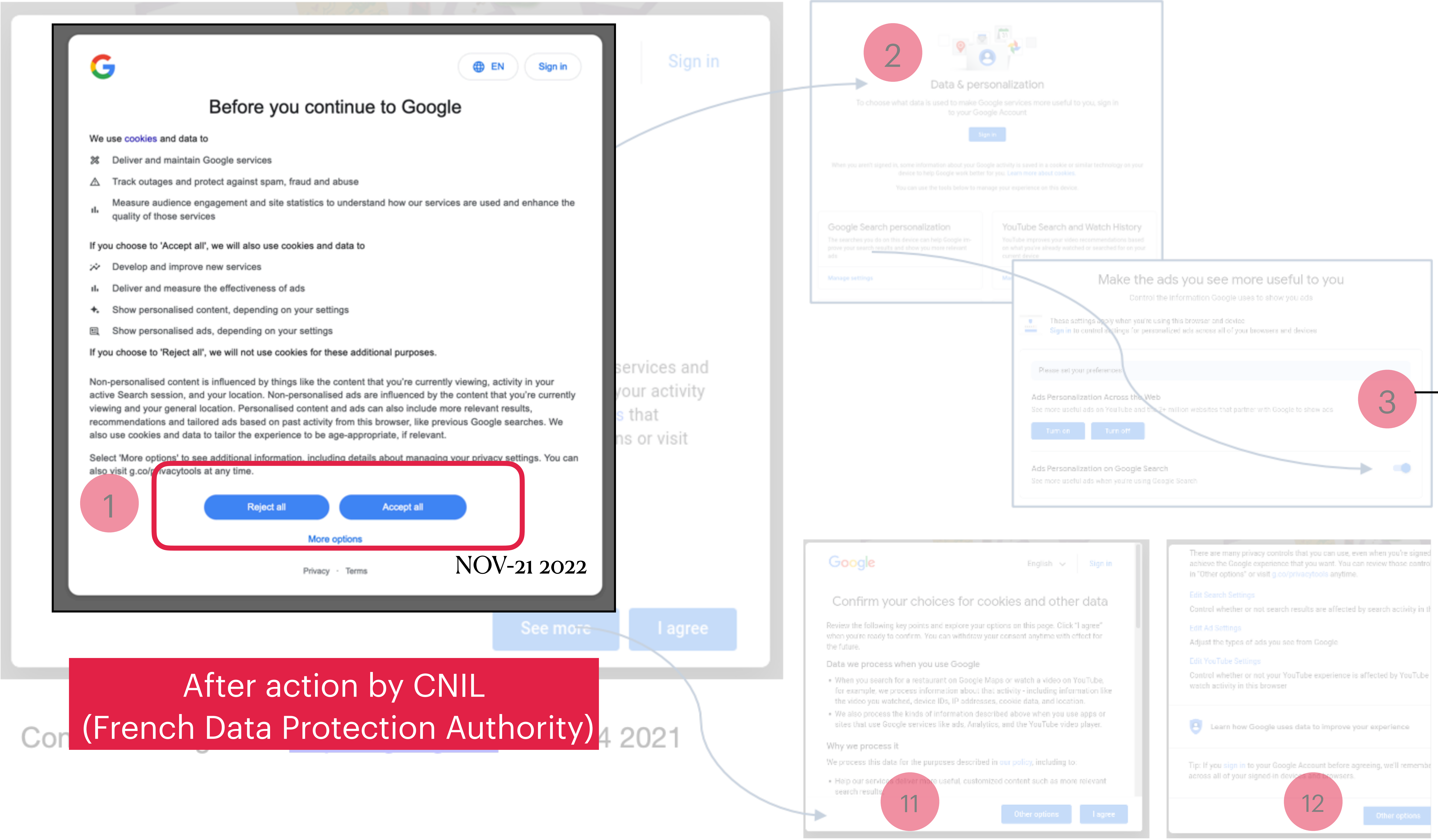
9

How many clicks to "Accept" ==> 1

How many clicks to "Reject" ==> 3

How many clicks to "Truly Reject" ==> 12

Do you think this is:
LEGAL ?
ETHICAL ?
NECESSARY ?



EN Sign in

Before you continue to Google

We use cookies and data to

- Deliver and maintain Google services
- Track outages and protect against spam, fraud and abuse
- Measure audience engagement and site statistics to understand how our services are used and enhance the quality of those services

If you choose to 'Accept all', we will also use cookies and data to

- Develop and improve new services
- Deliver and measure the effectiveness of ads
- Show personalised content, depending on your settings
- Show personalised ads, depending on your settings

If you choose to 'Reject all', we will not use cookies for these additional purposes.

Non-personalised content is influenced by things like the content that you're currently viewing, activity in your active Search session, and your location. Non-personalised ads are influenced by the content that you're currently viewing and your general location. Personalised content and ads can also include more relevant results, recommendations and tailored ads based on past activity from this browser, like previous Google searches. We also use cookies and data to tailor the experience to be age-appropriate, if relevant.

Select 'More options' to see additional information, including details about managing your privacy settings. You can also visit g.co/privacytools at any time.

Reject all | Accept all

More options

Privacy · Terms

NOV-21 2022

After action by CNIL
(French Data Protection Authority)

Data & personalization

To choose what data is used to make Google services more useful to you, sign in to your Google Account

Sign in

When you aren't signed in, some information about your Google activity is saved in a cookie or similar technology on your device to help Google work better for you. Learn more about cookies.

You can use the tools below to manage your experience on this device.

Google Search personalization

The searches you do on this device can help Google improve your search results and show you more relevant ads

Manage settings

YouTube Search and Watch History

YouTube improves your video recommendations based on what you've already watched or searched for on your current device

Make the ads you see more useful to you

Control the information Google uses to show you ads

These settings apply when you're using this browser and device
Sign in to control settings for personalized ads across all of your browsers and devices

Please set your preferences

Ads Personalization Across the Web

See more useful ads on YouTube and the 2+ million websites that partner with Google to show ads

Turn on | Turn off

Ads Personalization on Google Search

See more useful ads when you're using Google Search

Google English Sign in

Confirm your choices for cookies and other data

Review the following key points and explore your options on this page. Click "I agree" when you're ready to confirm. You can withdraw your consent anytime with effect for the future.

Data we process when you use Google

- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity - including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it

We process this data for the purposes described in our policy, including to:

- Help our services deliver more useful, customized content such as more relevant search results;

Other options | I agree

There are many privacy controls that you can use, even when you're signed
achieve the Google experience that you want. You can review those contro
in "Other options" or visit g.co/privacytools anytime.

Edit Search Settings

Control whether or not search results are affected by search activity in th

Edit Ad Settings

Adjust the types of ads you see from Google

Edit YouTube Settings

Control whether or not your YouTube experience is affected by YouTube watch activity in this browser

Learn how Google uses data to improve your experience

Tip: If you sign in to your Google Account before agreeing, we'll rememb
across all of your signed-in devices and browsers.

Other options

Companies are required to show you a "NOTICE" informing what data they collect and how they use it.

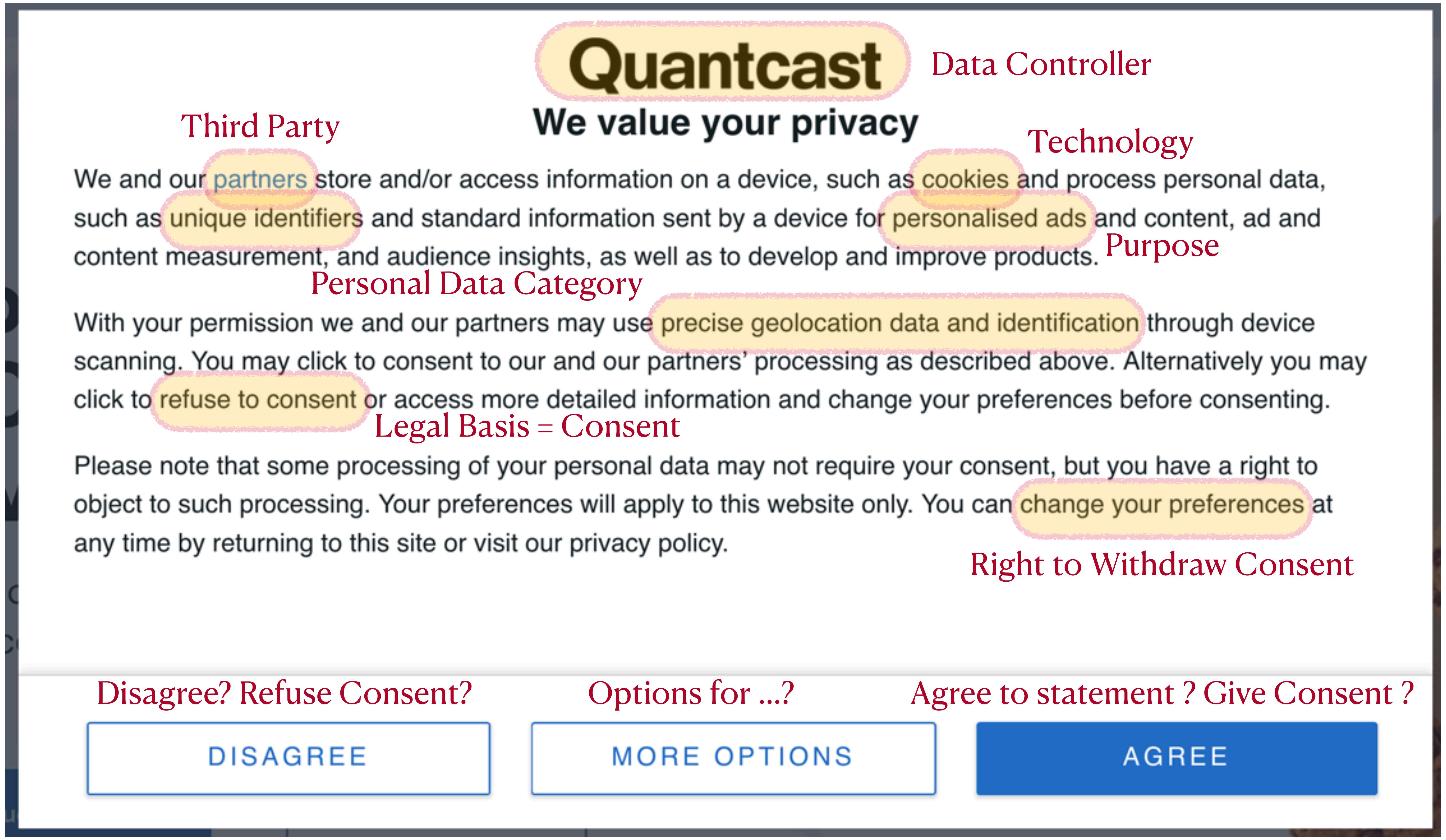
Where this is based on your CONSENT, they need to ask your permission before they can proceed.

Since every website visit collects and uses your personal data, this means there's a notice & consent process every time you visit a website ...

How many clicks to "Accept" ==> 1

How many clicks to "Reject" ==> 2

Hidden Gotches ? Several



Quantcast

Data Controller

We value your privacy

Third Party

Technology

We and our partners store and/or access information on a device, such as cookies and process personal data, such as unique identifiers and standard information sent by a device for personalised ads and content, ad and content measurement, and audience insights, as well as to develop and improve products.

Purpose

Personal Data Category

With your permission we and our partners may use precise geolocation data and identification through device scanning. You may click to consent to our and our partners' processing as described above. Alternatively you may click to refuse to consent or access more detailed information and change your preferences before consenting.

Legal Basis = Consent

Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing. Your preferences will apply to this website only. You can change your preferences at any time by returning to this site or visit our privacy policy.

Right to Withdraw Consent

Disagree? Refuse Consent?

Options for ...?

Agree to statement ? Give Consent ?

https://www.quantcast.com/ THU 17 NOV 2021

What is your first impulse to do here?
What button do you think you would have clicked?
What button do you think most people click?

GDPR Art 4, 7, 13, 14

Information to be provided in a "Notice"

- Identity of Controller
- Purpose
- Processing Categories
- Personal Data Categories
- Right to Withdraw Consent
- Data Storage Periods
- Data Sharing / Recipients
- Trans-border data flows
- Technical and Org. Measures
- Risks envisioned (sic.)
- Automated Decision Making
- Novel technologies
- Profiling / Surveillance (sic.)

Consent should be:

1. Freely given → without coercion, no obligation
2. Specific → exact and limited in scope
3. Informed → prior knowledge about consequences
4. Un-ambigious → clear indication of consenting
5. Revocable/Withdrawable → can be "cancelled"

Sometimes it outright illegal !!!

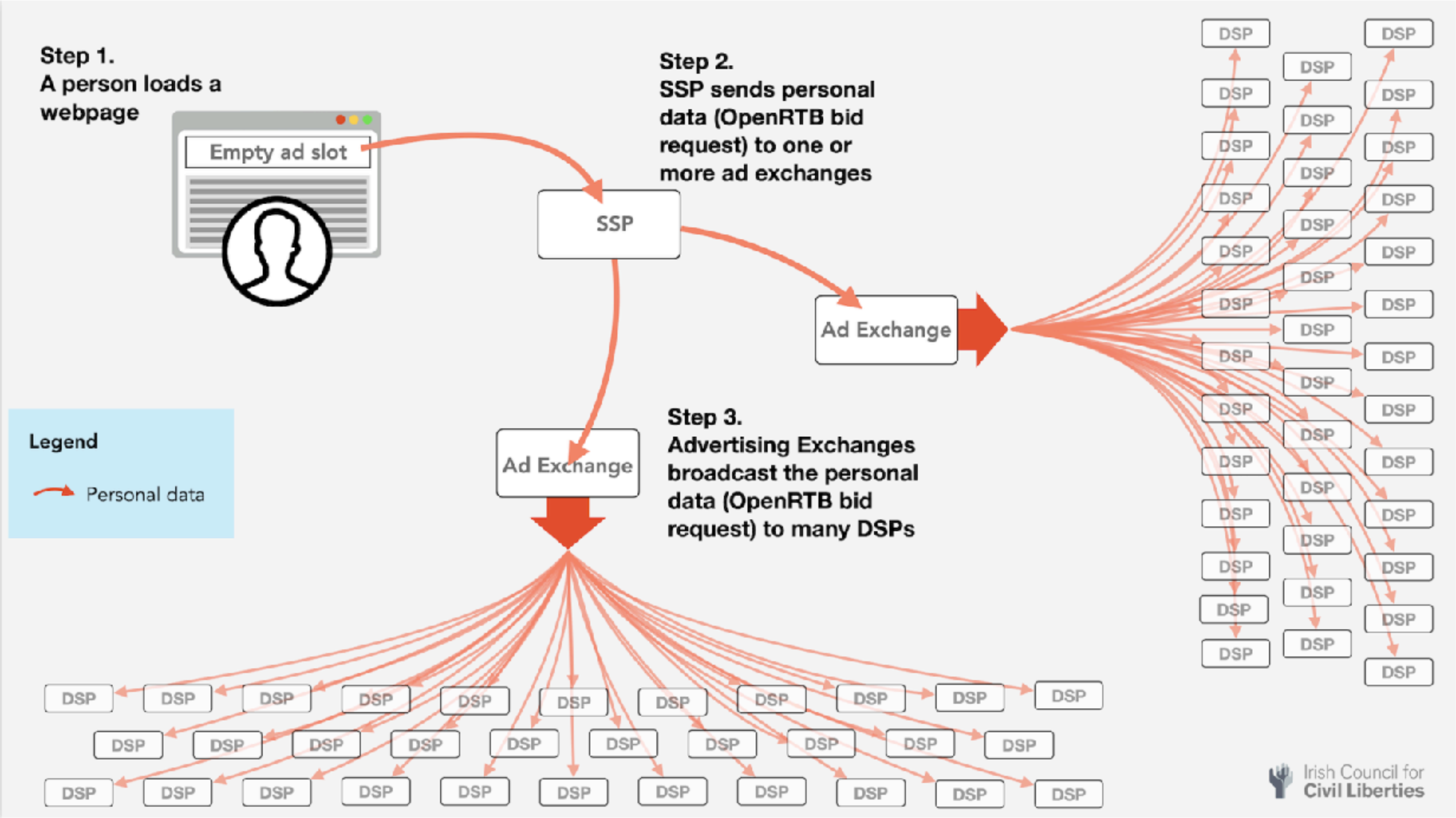
- Consent "assumed" even before you make a choice [1]
- Consent "assumed" even if you click disagree [1]
- Incorrect use of legal base e.g. use Legitimate Interest instead of consent [2]
- Collect consent for ~1000 third parties with a single click [2]
- Make it difficult to withdraw consent [2]
- Keep fighting court cases instead of fixing obviously illegal practices [3]

[1] For example, see Nouwens, Midas, et al. "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence." *Proceedings of the 2020 CHI conference on human factors in computing systems*. 2020. https://people.csail.mit.edu/ilaria/papers/Midas-MITCHI2020.pdf

[2] Matte, Célestin, Nataliia Bielova, and Cristiana Santos. "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework." 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020. https://hal.inria.fr/hal-03117294/document

[3] See investigation reports and documents published regarding WhatsApp v DPC Ireland and Facebook/Meta v DPC Ireland (2021)

Personalised Advertising via Real-Time Bidding


Step 1.
A person loads a webpage
Empty ad slot
SSP
Step 2.
SSP sends personal data (OpenRTB bid request) to one or more ad exchanges
Ad Exchange
Ad Exchange
Step 3.
Advertising Exchanges broadcast the personal data (OpenRTB bid request) to many DSPs
Legend
Personal data
DSP
Irish Council for Civil Liberties

https://www.iccl.ie/digital-data/iab-europe-cant-audit-what-1000-companies-that-use-its-tcf-system-do-with-our-personal-data/

Overview of Personalisation Issues

Key takeaways

- What data is 'used' ??? —> Transparency
- What data is 'needed'? What is 'necessary'? —> Data Minimisation
- What are the sources of 'data' ? —> Transparency
- Is any data 'sensitive' ? Is it 'special' ? —> Ethical Concerns
- Is data (input/output) 'accurate' —> Accountability
- Is the output configurable ? —> Privacy by Design / Default
- Understand distinctions between *Privacy* vs *Security* vs *Identifiability* vs *Control*

SOLID: A Decentralised Web

https://solidproject.org/

Centralised

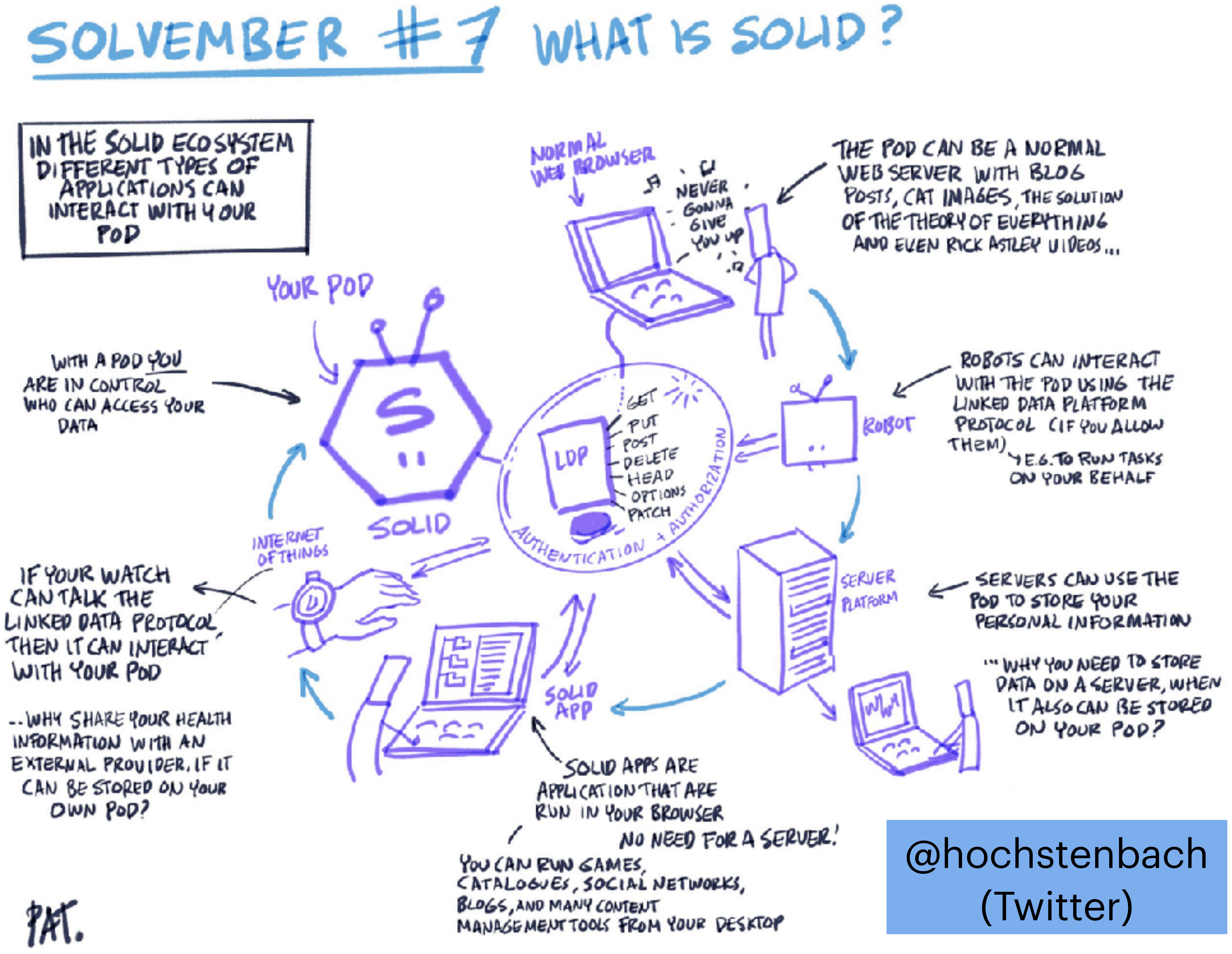
- ○ Companies decide how to collect, store data
- ○ Companies decide how/where to use it
- ○ Companies offer you choices and controls

Decentralised

- ○ You “control” where your data is stored
- ○ You “control” how it is used by apps/services
- ○ You offer choices and controls

What will SOLID need to work?

- ○ A new way to express privacy and preferences
- ○ User-friendly UI/UX *without dark patterns*
- ○ Legal enforcement to make companies respect negotiation of user preferences and settings


SOLVEMBER #7 WHAT IS SOLID?
IN THE SOLID ECOSYSTEM DIFFERENT TYPES OF APPLICATIONS CAN INTERACT WITH YOUR POD
NORMAL WEB BROWSER
NEVER GONNA GIVE YOU UP
THE POD CAN BE A NORMAL WEB SERVER WITH BLOG POSTS, CAT IMAGES, THE SOLUTION OF THE THEORY OF EVERYTHING AND EVEN RICK ASTLEY VIDEOS...
YOUR POD
WITH A POD YOU ARE IN CONTROL WHO CAN ACCESS YOUR DATA
S
SOLID
LDP
GET
PUT
POST
DELETE
HEAD
OPTIONS
PATCH
AUTHENTICATION + AUTHORIZATION
ROBOT
ROBOTS CAN INTERACT WITH THE POD USING THE LINKED DATA PLATFORM PROTOCOL (IF YOU ALLOW THEM)
E.G. TO RUN TASKS ON YOUR BEHALF
INTERNET OF THINGS
IF YOUR WATCH CAN TALK THE LINKED DATA PROTOCOL, THEN IT CAN INTERACT WITH YOUR POD
..WHY SHARE YOUR HEALTH INFORMATION WITH AN EXTERNAL PROVIDER, IF IT CAN BE STORED ON YOUR OWN POD?
SOLID APP
SOLID APPS ARE APPLICATION THAT ARE RUN IN YOUR BROWSER
NO NEED FOR A SERVER!
YOU CAN RUN GAMES, CATALOGUES, SOCIAL NETWORKS, BLOGS, AND MANY CONTENT MANAGEMENT TOOLS FROM YOUR DESKTOP
SERVER PLATFORM
SERVERS CAN USE THE POD TO STORE YOUR PERSONAL INFORMATION
...WHY YOU NEED TO STORE DATA ON A SERVER, WHEN IT ALSO CAN BE STORED ON YOUR POD?
PAT.

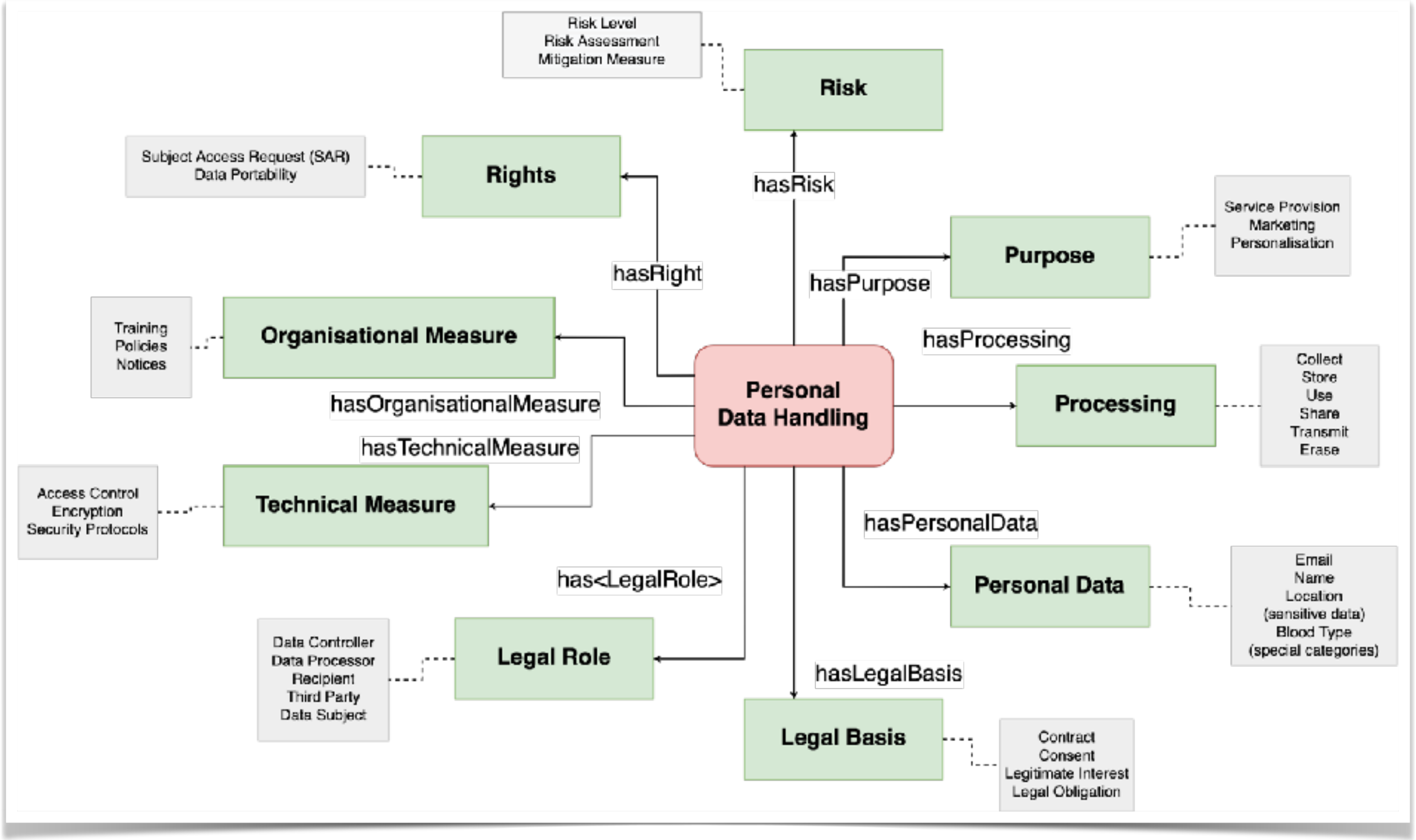
@hochstenbach
(Twitter)

What am I working on?

Privacy Risks, GDPR, Legal Compliance, Semantics

Machine-Readable Metadata for Automated Approaches

Data Privacy Vocabulary (DPV) https://w3id.org/dpv



The Data Privacy Vocabulary (DPV) reflects ~5 years of efforts in creating an open resource providing concepts related to personal data processing, privacy, data protection, and GDPR

DPV's taxonomies provide semantic interoperability, which enables new, innovative, smart, and automated solutions

Demonstrated usefulness for important use-cases, e.g. ROPA, consent, compliance checking

We're looking to the future! DGA / ePR / AI-Act / Data Spaces

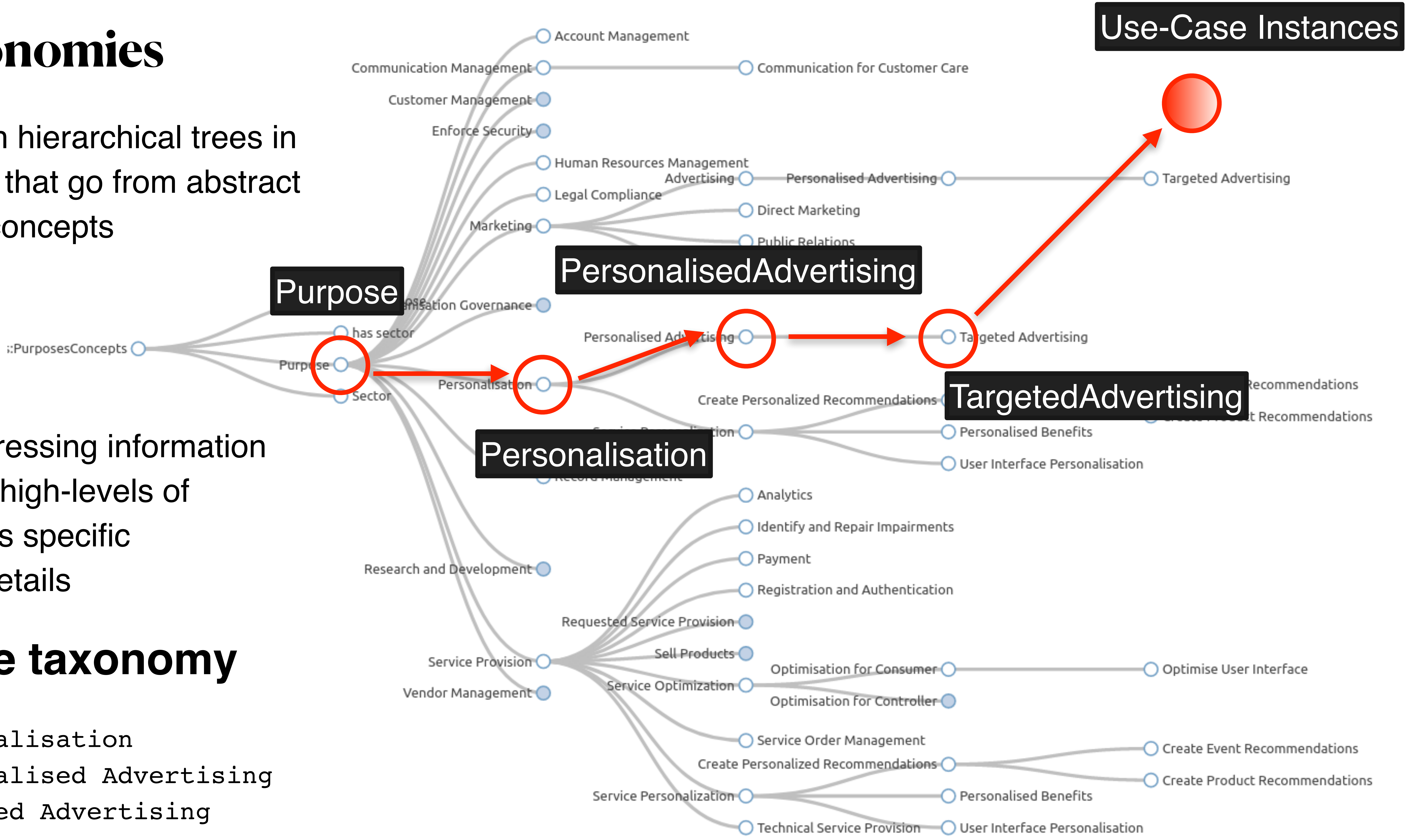
DPV Taxonomies

DPV provides rich hierarchical trees in top-down fashion that go from abstract to more specific concepts

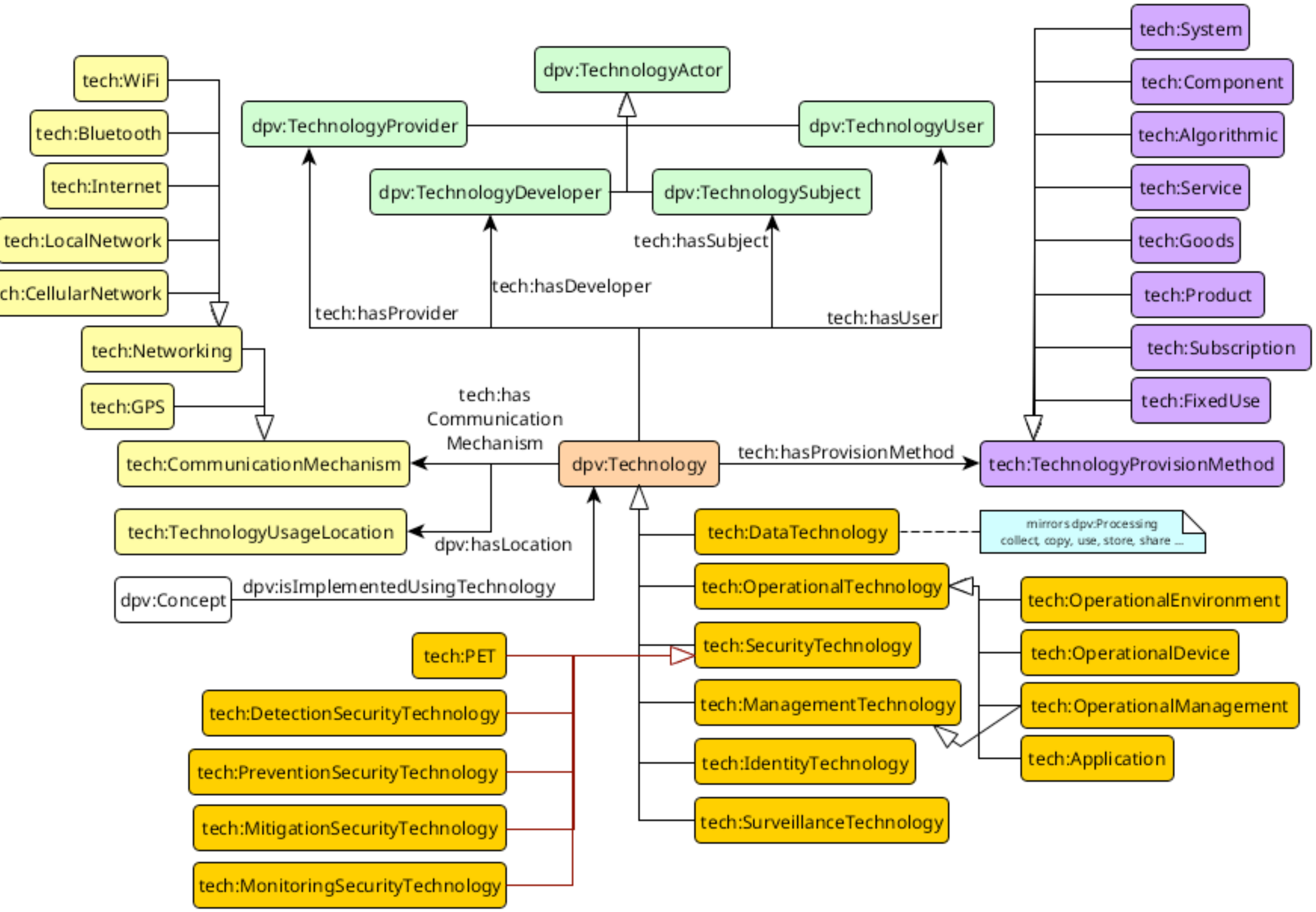
This enables expressing information and rules at both high-levels of abstraction and as specific implementation details

E.g. Purpose taxonomy

```
Purpose → Personalisation
        → Personalised Advertising
        → Targeted Advertising
```



generated by SKOSPlay https://skos-play.sparna.fr/



A ‘Model’ of Technologies

DPV TECH extension
https://w3id.org/dpv/tech

DPV Applications

current work

1. Register of Processing Activities (ROPA)
2. Consent Records
3. Compliance Checking
4. Impact Assessments (PIA / DPIA)
5. Data Input/Output Assistance
6. Annotating code / documents
7. Expressing and Evaluating Rules

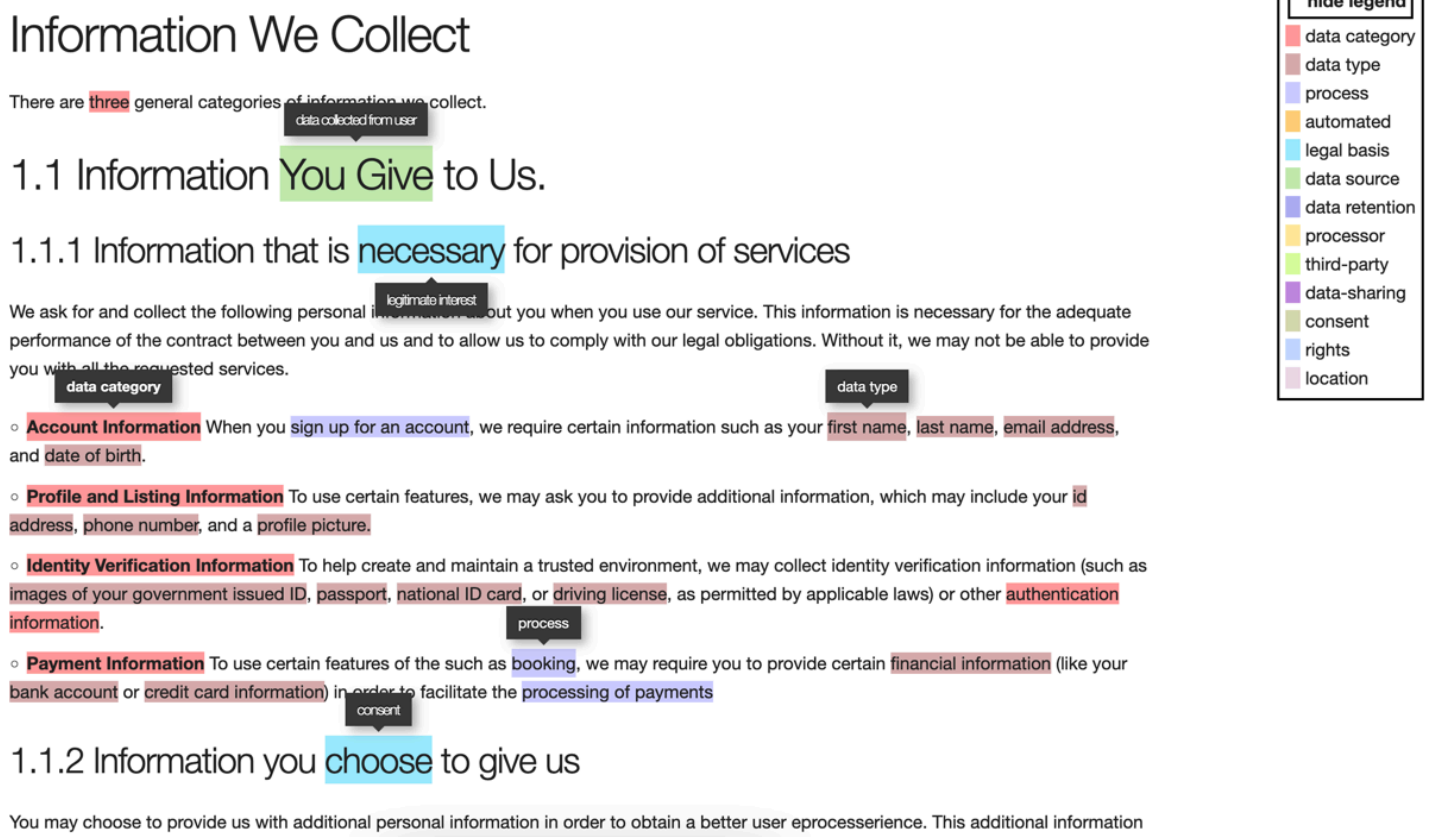
work in progress

1. Risk Management
2. Data Breach Records
3. Subject Access Request
4. Data Portability
5. Data Transfers
6. Privacy Policies
7. Standards & Guidelines

Real-World Use-Cases

Privacy Policy Analysis

https://openscience.adaptcentre.ie/privacy-policy/personalise/demo/policy.html



Information We Collect

There are three general categories of information we collect.

1.1 Information You Give to Us.

1.1.1 Information that is necessary for provision of services

We ask for and collect the following personal information about you when you use our service. This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations. Without it, we may not be able to provide you with all the requested services.

- **Account Information** When you sign up for an account, we require certain information such as your first name, last name, email address, and date of birth.
- **Profile and Listing Information** To use certain features, we may ask you to provide additional information, which may include your id address, phone number, and a profile picture.
- **Identity Verification Information** To help create and maintain a trusted environment, we may collect identity verification information (such as images of your government issued ID, passport, national ID card, or driving license, as permitted by applicable laws) or other authentication information.
- **Payment Information** To use certain features of the such as booking, we may require you to provide certain financial information (like your bank account or credit card information) in order to facilitate the processing of payments

1.1.2 Information you choose to give us

You may choose to provide us with additional personal information in order to obtain a better user eprocesserience. This additional information

GDPR

Regulating Processing of Personal Data

Harshvardhan J. Pandit
harshvardhan.pandit@dcu.ie

CA349 IT Architecture | DCU
Slides available at: https://harshp.com/research/presentations