GDPR

Regulating Processing of Personal Data

Harshvardhan J. Pandit
pandith@tcd.ie | @coolharsh55

Regulating Big Tech - Utrecht Uni. | 20 December 2021 | Online/Virtual
Slides available at: https://harshp.com/research/presentations

Harsh(vardhan J. Pandit)

An Introduction

- Postdoctoral Researcher at Trinity College Dublin, IE
- Current Project: creating a knowledge graph of privacy risks for DPIA
- 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)

Personal Data

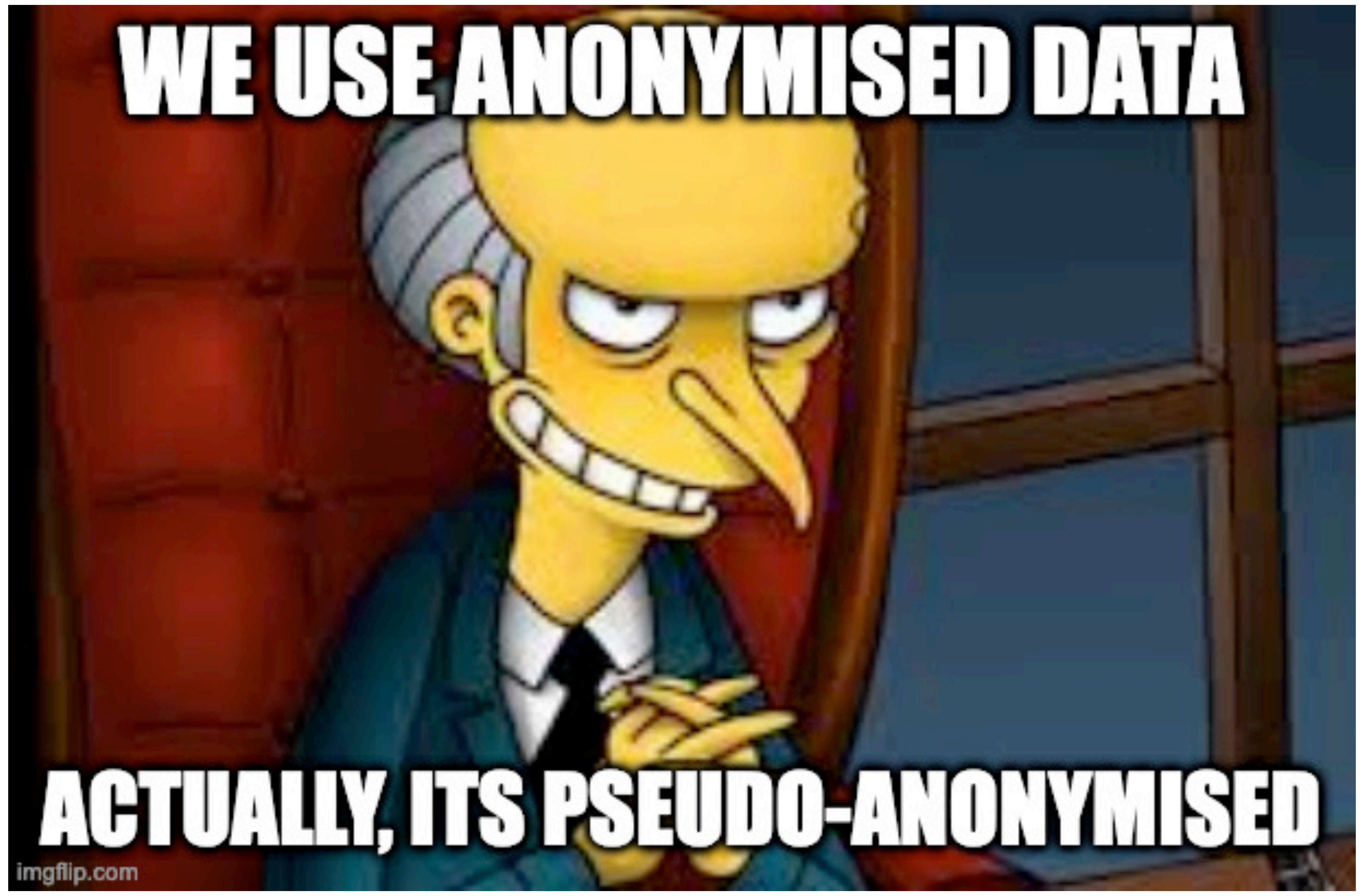
Identifiers, and Identifiability

1. Identifiers: Harsh (name), pandith@tcd.ie (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

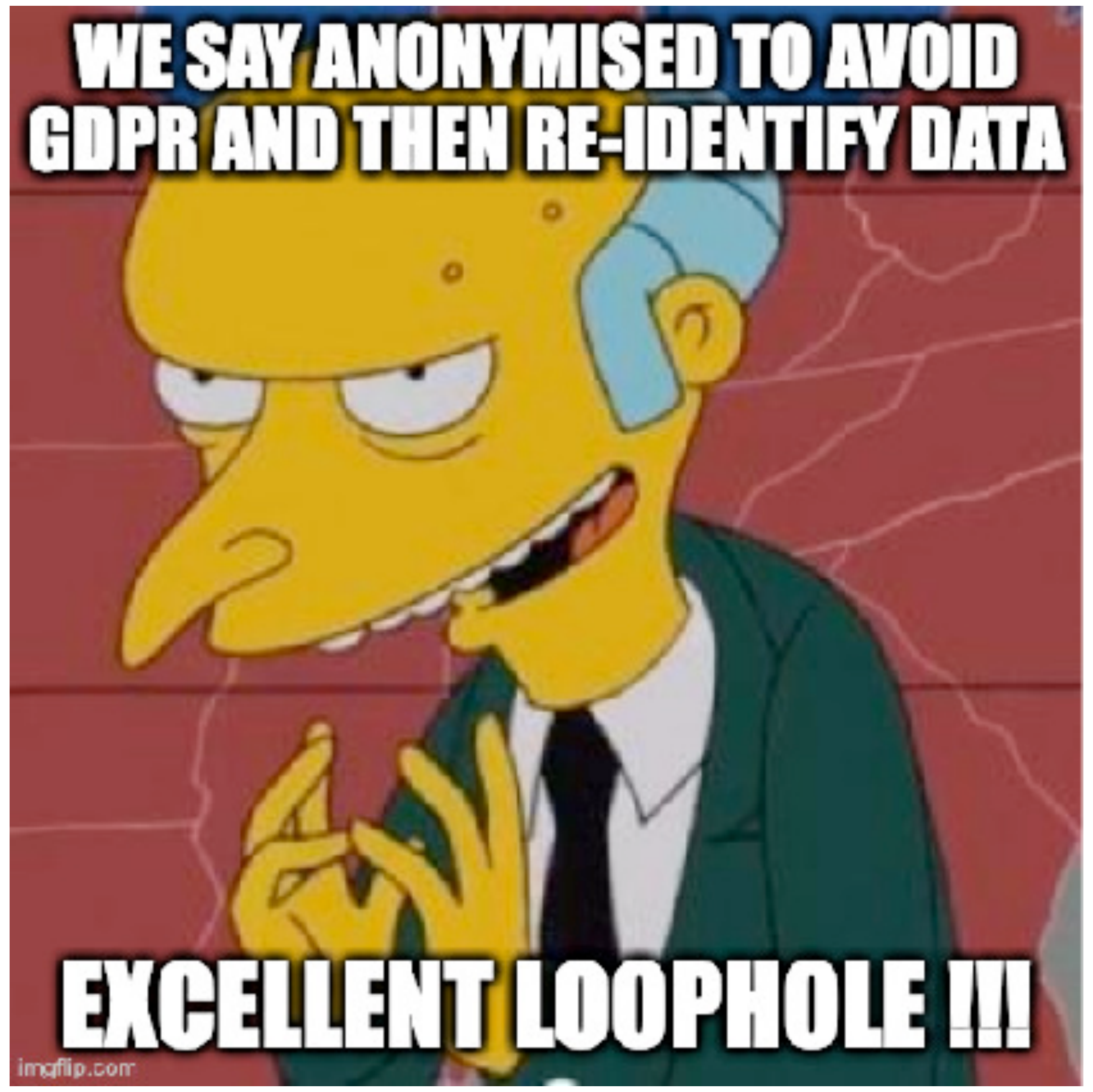
- Anonymisation is the removal of (some) 'identifying' attributes from data
- Merely using "**anonymisation**" does not produce anonymised data
- It produces '**pseudo-anonmised**' data, which is still personal data
- 'Completely anonymised' if it is **not identifiable**
- E.g.
  - Your exact location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

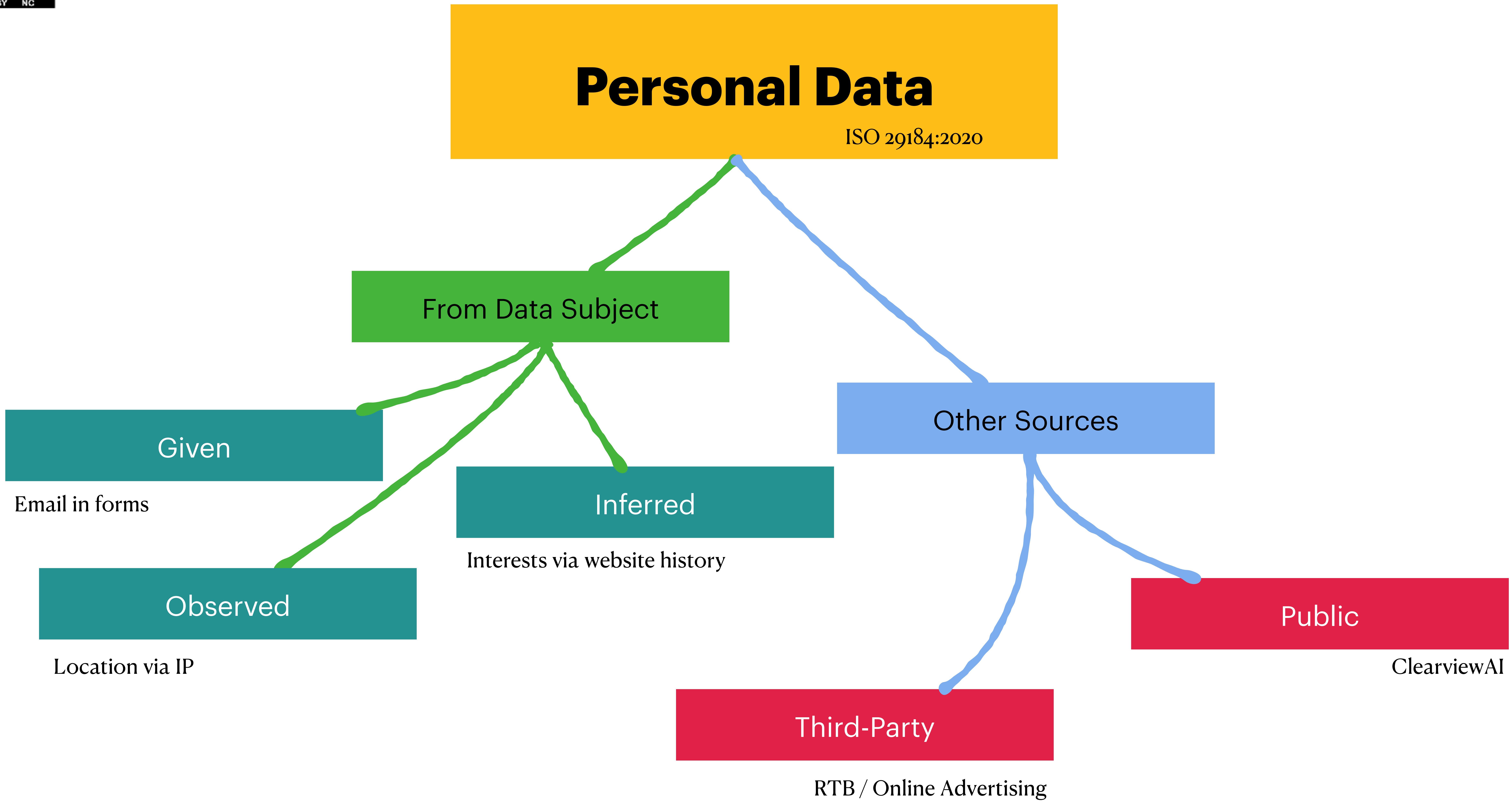


Q: When is Anonymised Data not Anonymised?

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

Processing Overview

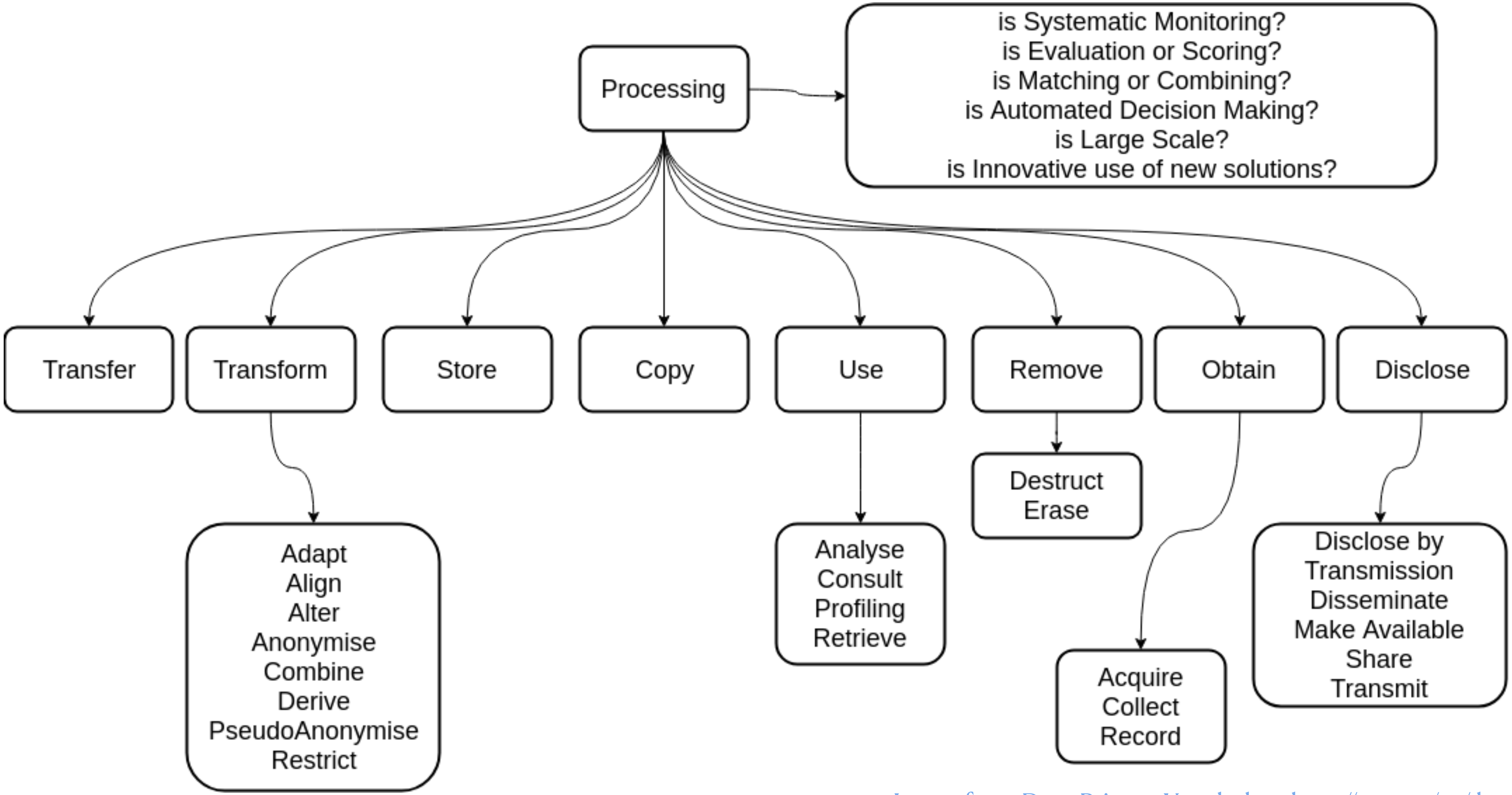


Image from Data Privacy Vocabulary http://w3.org/ns/dpv

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

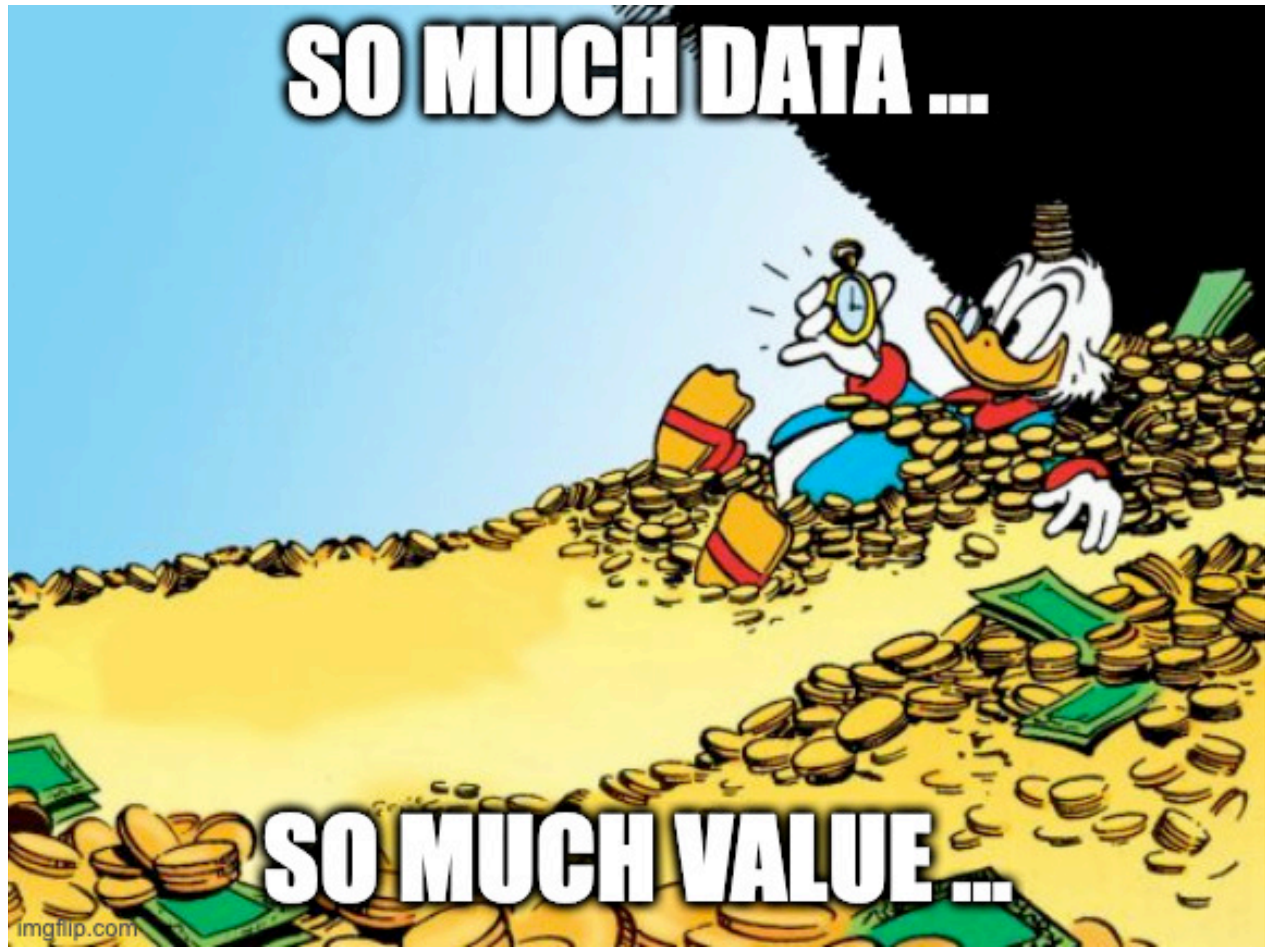
Purpose

GDPR

All Processing in GDPR *must* be towards a Goal

Implied when a ‘Purpose’ is necessary as per Article.5

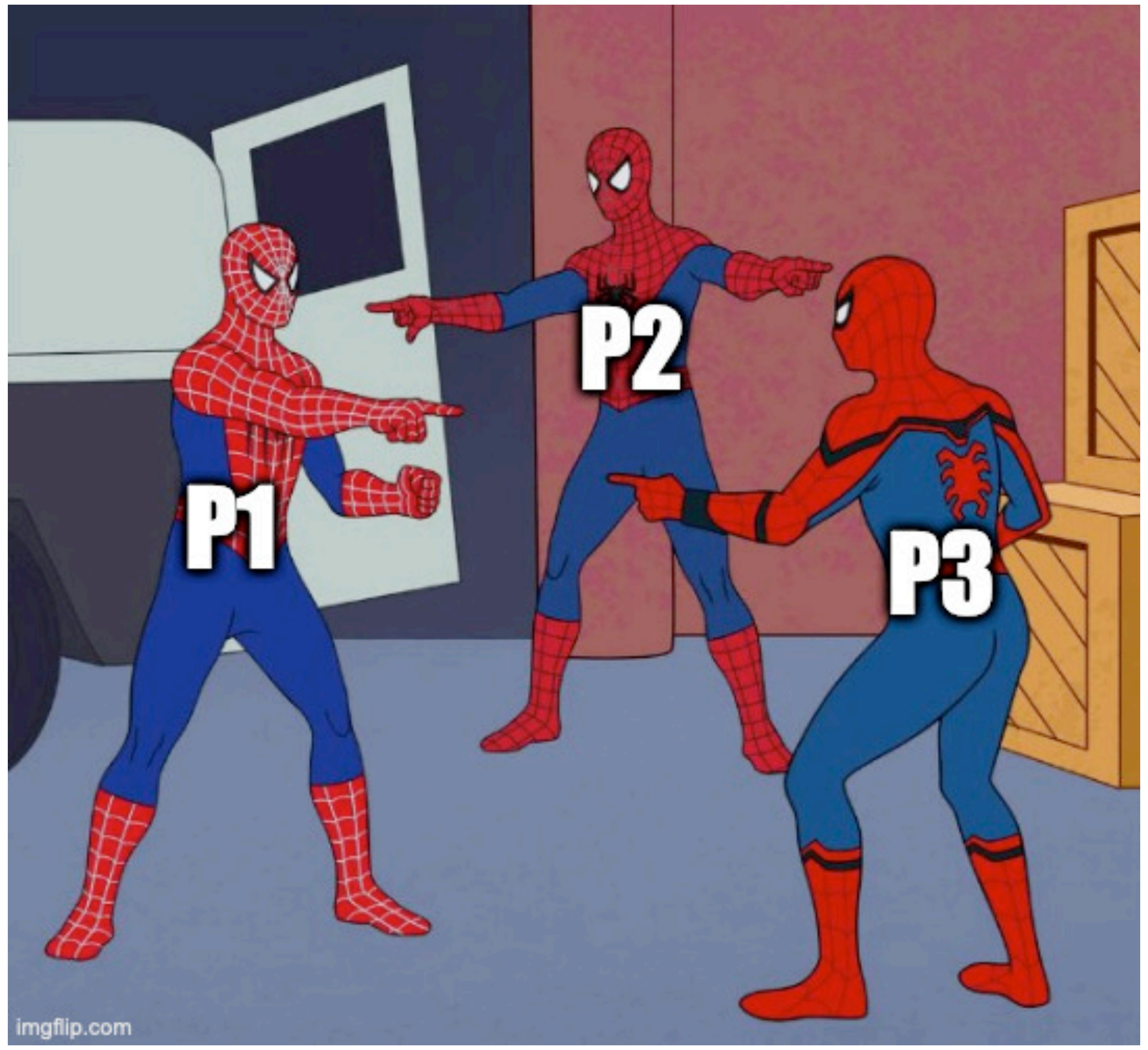
Every Processing *must* have a Purpose



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

Purposes must be *specific* and *unambiguous*

Purposes must be separate from other matter, including other purposes



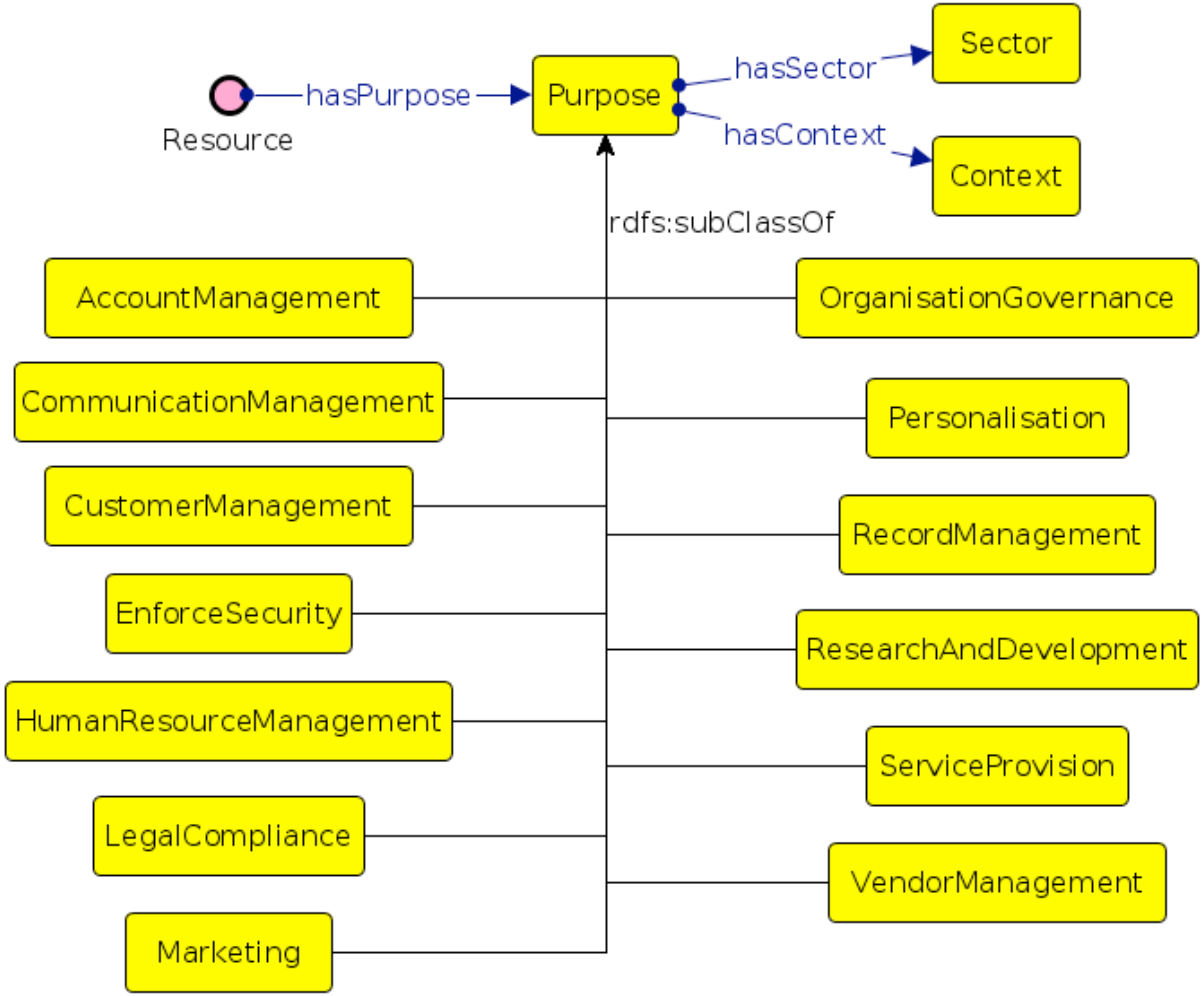
Purposes are intended to be human-readable and human-comprehensible

Purposes should not be broad and abstract

Purposes should be specific and contextual to their use-case

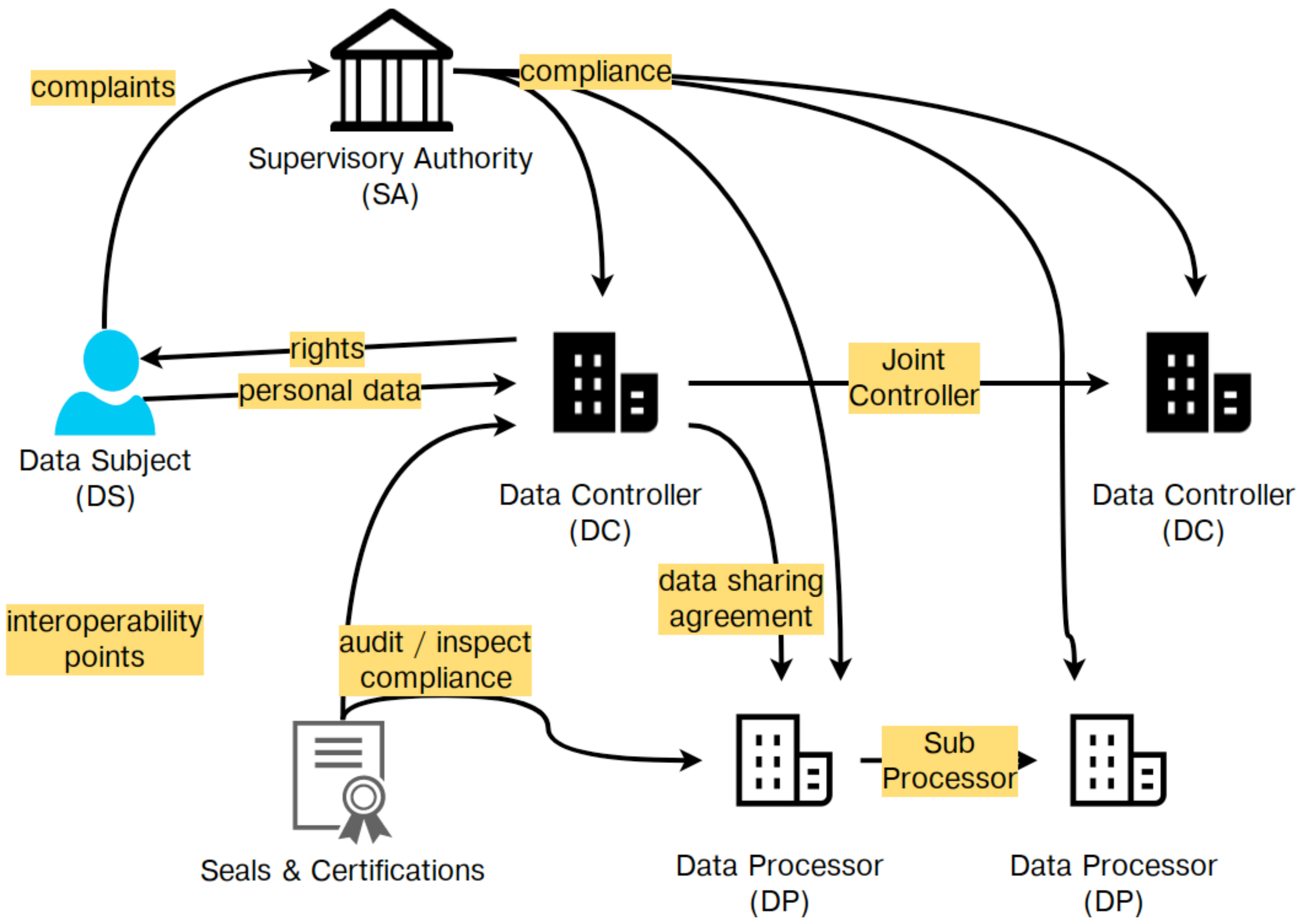
Purposes can be grouped or categorised, but not replaced, e.g. with Marketing for 'Sending new product emails'

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)

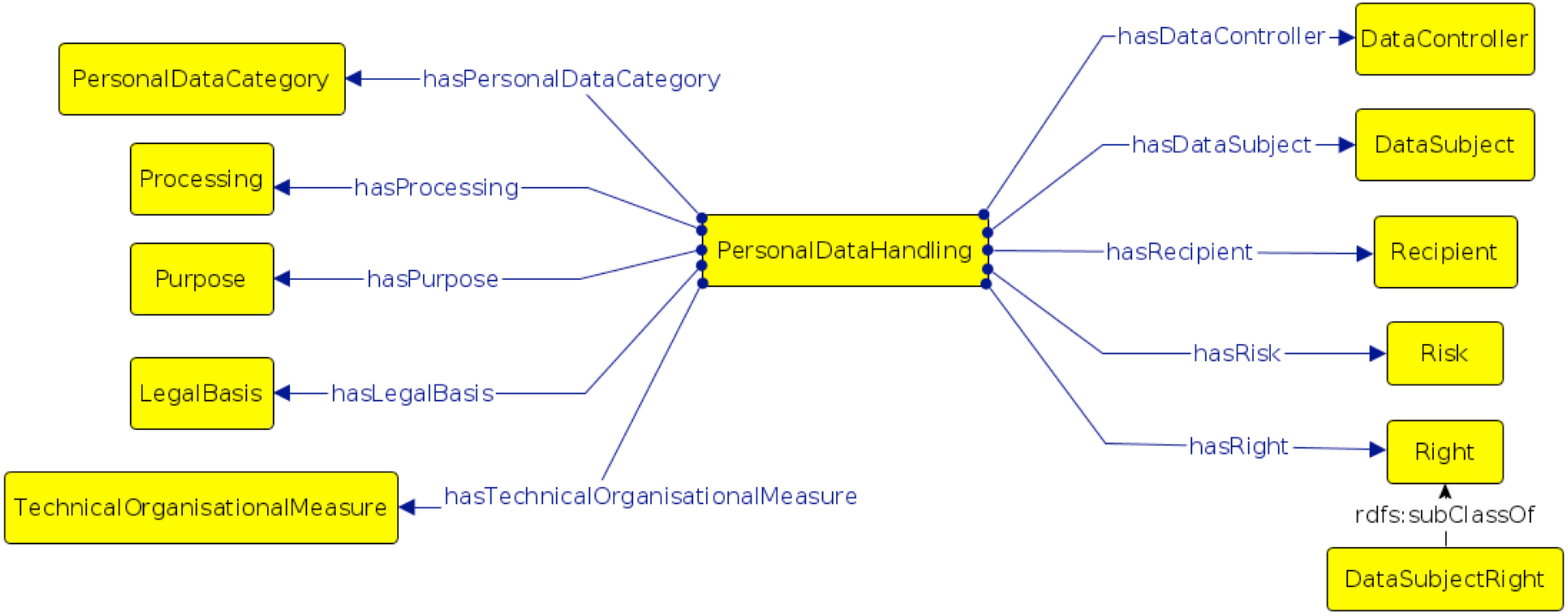
A12-A22 Rights
Transparency (A.12)
Notice (A.13, A.14) ;
Object to Processing
Rectification of Data
Erasure (Right to be Forgotten)
Restriction of Processing
Right of Access
Data Portability

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

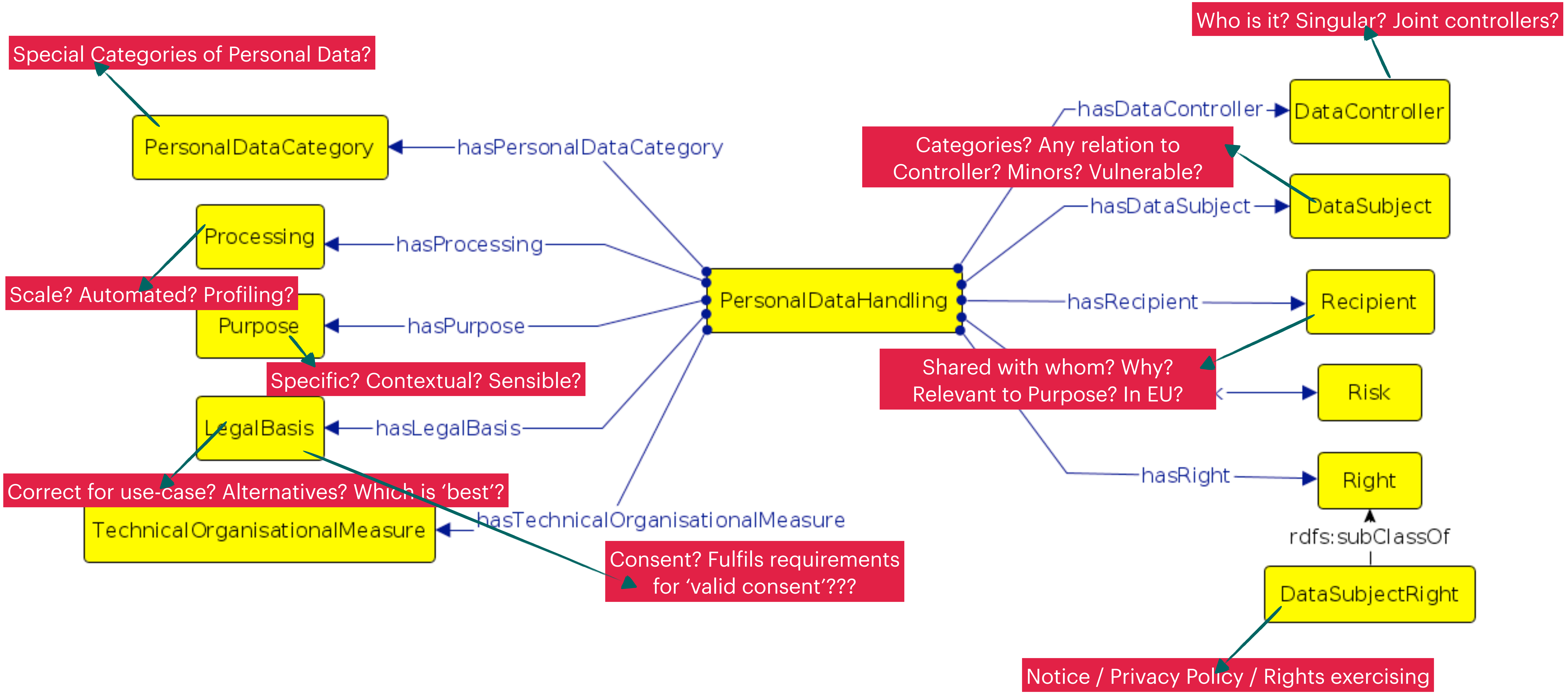
Investigating ‘Personal Data Handling’

GDPR

Step 1: Identify concepts for the use-case



Step 2: Compare against requirements

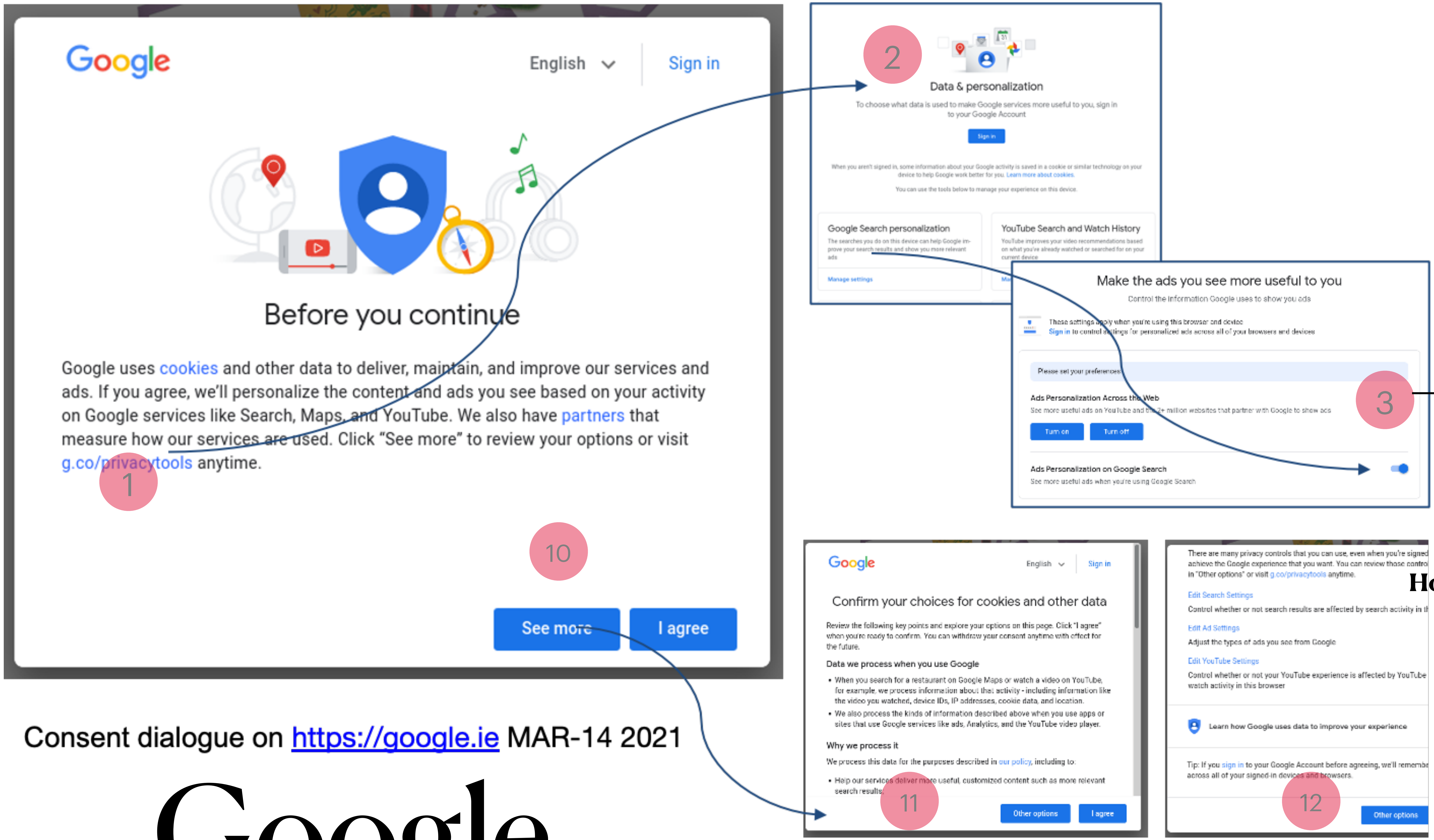

Who is it? Singular? Joint controllers?
Special Categories of Personal Data?
hasDataController
DataController
PersonalDataCategory
hasPersonalDataCategory
Categories? Any relation to Controller? Minors? Vulnerable?
hasDataSubject
DataSubject
Processing
hasProcessing
PersonalDataHandling
hasRecipient
Recipient
Scale? Automated? Profiling?
Purpose
hasPurpose
Shared with whom? Why? Relevant to Purpose? In EU?
Risk
Specific? Contextual? Sensible?
LegalBasis
hasLegalBasis
hasRight
Right
Correct for use-case? Alternatives? Which is 'best'?
hasTechnicalOrganisationalMeasure
TechnicalOrganisationalMeasure
rdfs:subClassOf
Consent? Fulfils requirements for 'valid consent'???
DataSubjectRight
Notice / Privacy Policy / Rights exercising

Break (10 mins)

We’ll be back here at 12:00 CET

What does BigTech do for GDPR??? Lets' find out!

We'll take a quick look at notices and policies by GAFAM = Google, Apple, Facebook, Amazon, Microsoft



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

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

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

Google

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" ==> 3

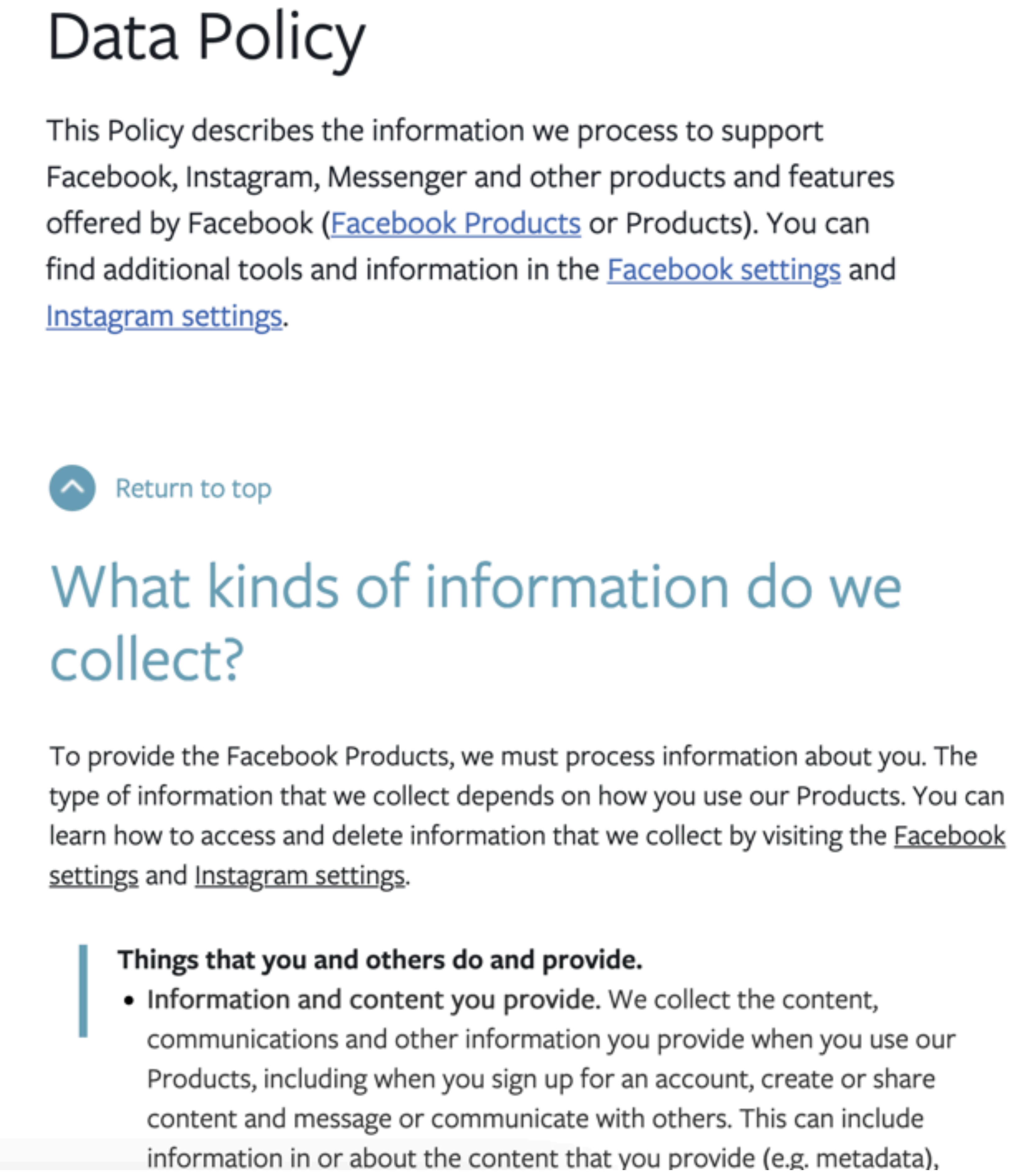
How many clicks to "Truly Reject" ==> 12

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

Facebook

https://www.facebook.com/legal/terms/update

https://www.facebook.com/about/privacy/update



Data Policy

This Policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook (Facebook Products or Products). You can find additional tools and information in the Facebook settings and Instagram settings.

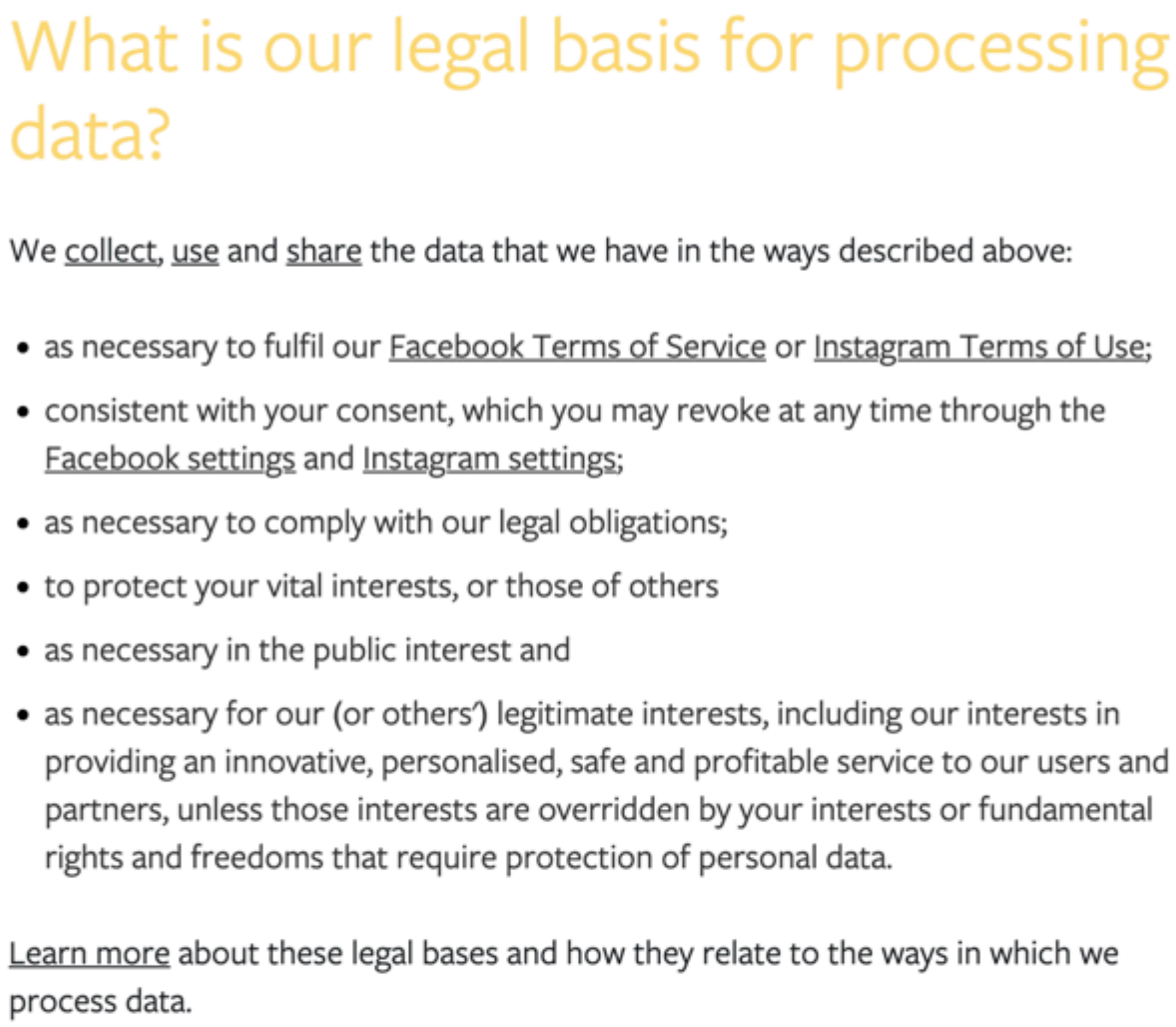
Return to top

What kinds of information do we collect?

To provide the Facebook Products, we must process information about you. The type of information that we collect depends on how you use our Products. You can learn how to access and delete information that we collect by visiting the Facebook settings and Instagram settings.

Things that you and others do and provide.

- **Information and content you provide.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content and message or communicate with others. This can include information in or about the content that you provide (e.g. metadata),

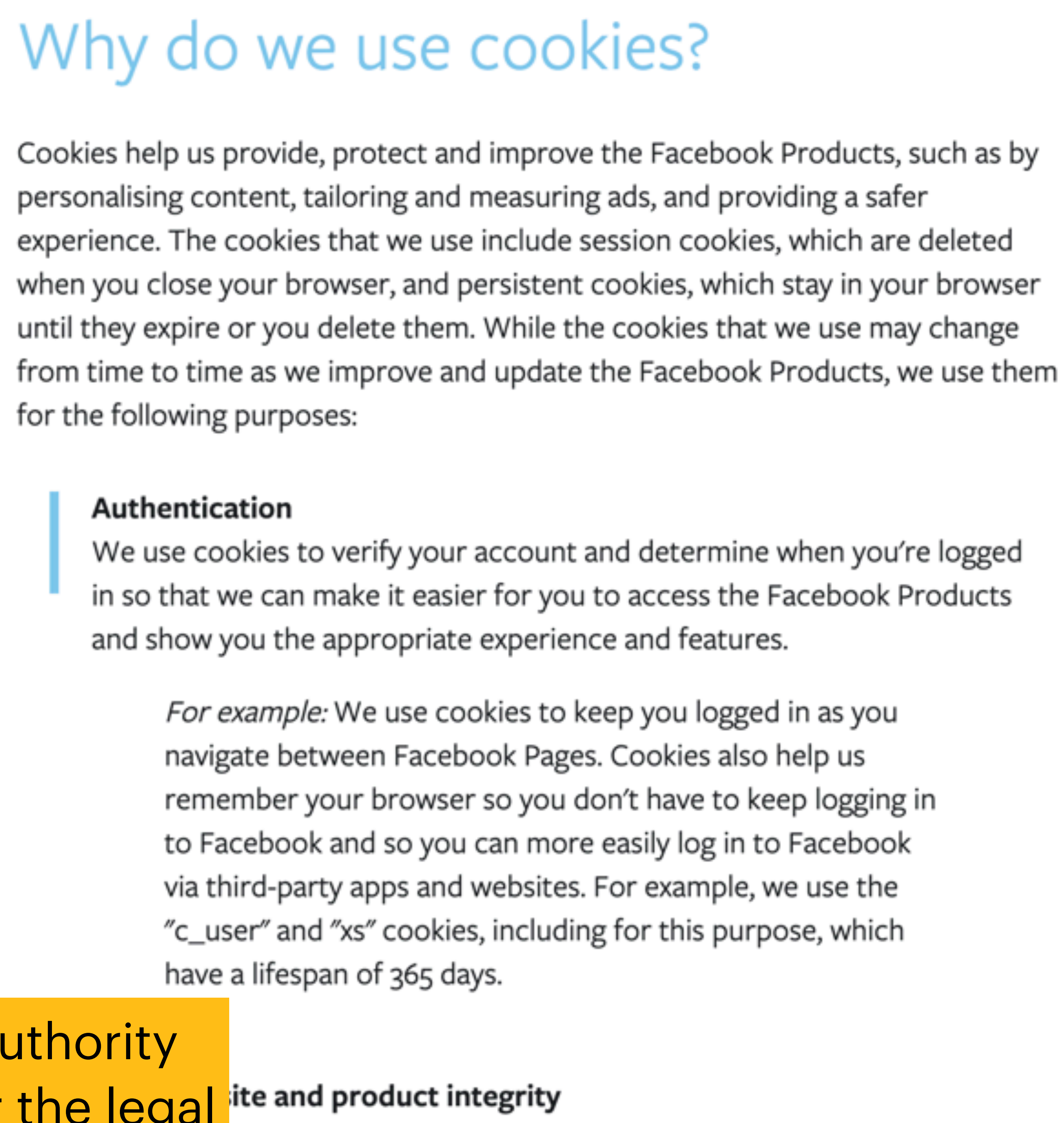


What is our legal basis for processing data?

We collect, use and share the data that we have in the ways described above:

- as necessary to fulfil our Facebook Terms of Service or Instagram Terms of Use;
- consistent with your consent, which you may revoke at any time through the Facebook settings and Instagram settings;
- as necessary to comply with our legal obligations;
- to protect your vital interests, or those of others
- as necessary in the public interest and
- as necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalised, safe and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data.

Learn more about these legal bases and how they relate to the ways in which we process data.



Why do we use cookies?

Cookies help us provide, protect and improve the Facebook Products, such as by personalising content, tailoring and measuring ads, and providing a safer experience. The cookies that we use include session cookies, which are deleted when you close your browser, and persistent cookies, which stay in your browser until they expire or you delete them. While the cookies that we use may change from time to time as we improve and update the Facebook Products, we use them for the following purposes:

Authentication

We use cookies to verify your account and determine when you're logged in so that we can make it easier for you to access the Facebook Products and show you the appropriate experience and features.

For example: We use cookies to keep you logged in as you navigate between Facebook Pages. Cookies also help us remember your browser so you don't have to keep logging in to Facebook and so you can more easily log in to Facebook via third-party apps and websites. For example, we use the "c_user" and "xs" cookies, including for this purpose, which have a lifespan of 365 days.

ite and product integrity

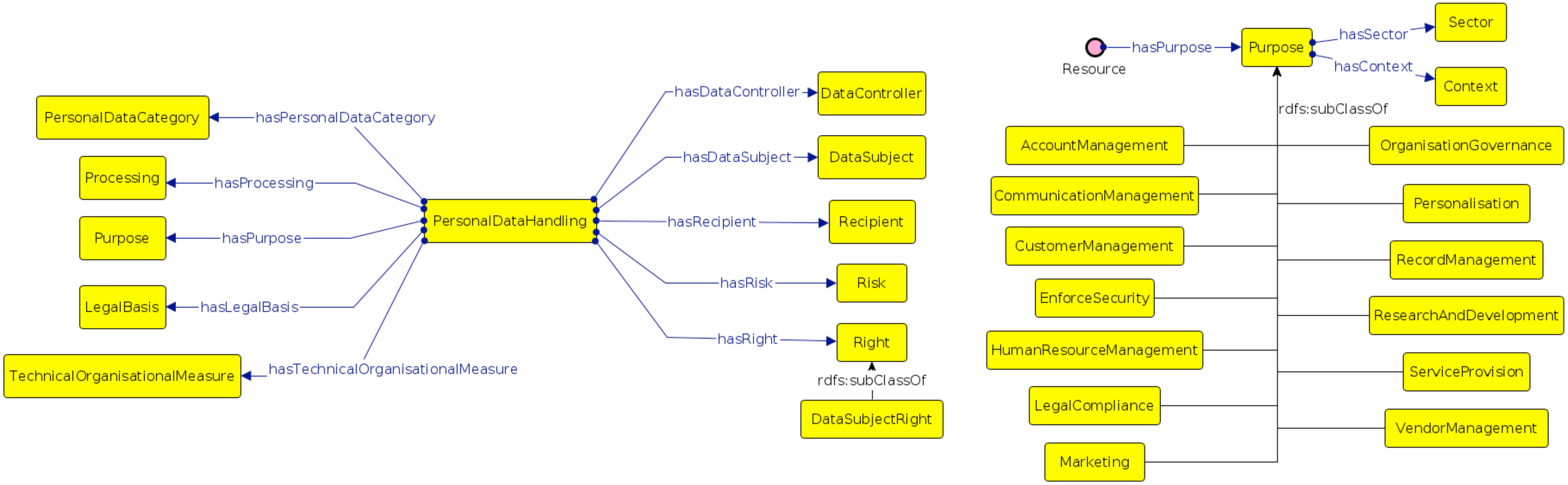
Note: Ongoing case with Irish Data Protection Authority filed by Max Schrems (NOYB) regarding whether the legal basis (contract) used by Facebook is the correct one to be used under GDPR. The basic argument is, Facebook claims personalised advertising is a necessary part of providing a social network service and what the users accept when they agree to the terms and conditions.

What am I working on?

Privacy Risks, GDPR, Legal Compliance, Semantics

Machine-Readable Metadata for Automated Approaches

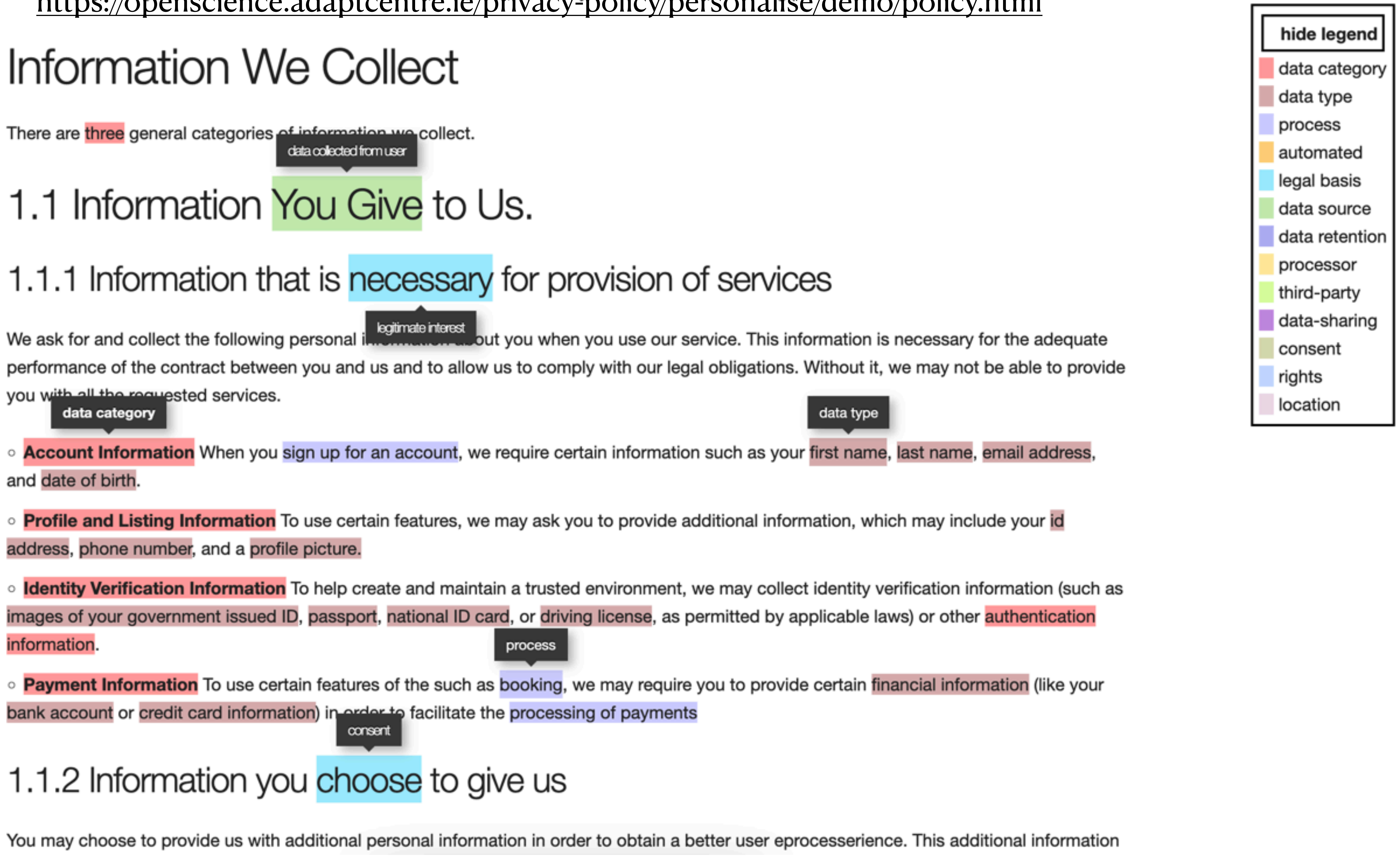
Data Privacy Vocabulary (DPV), v0.3, 2021 https://w3.org/ns/dpv



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

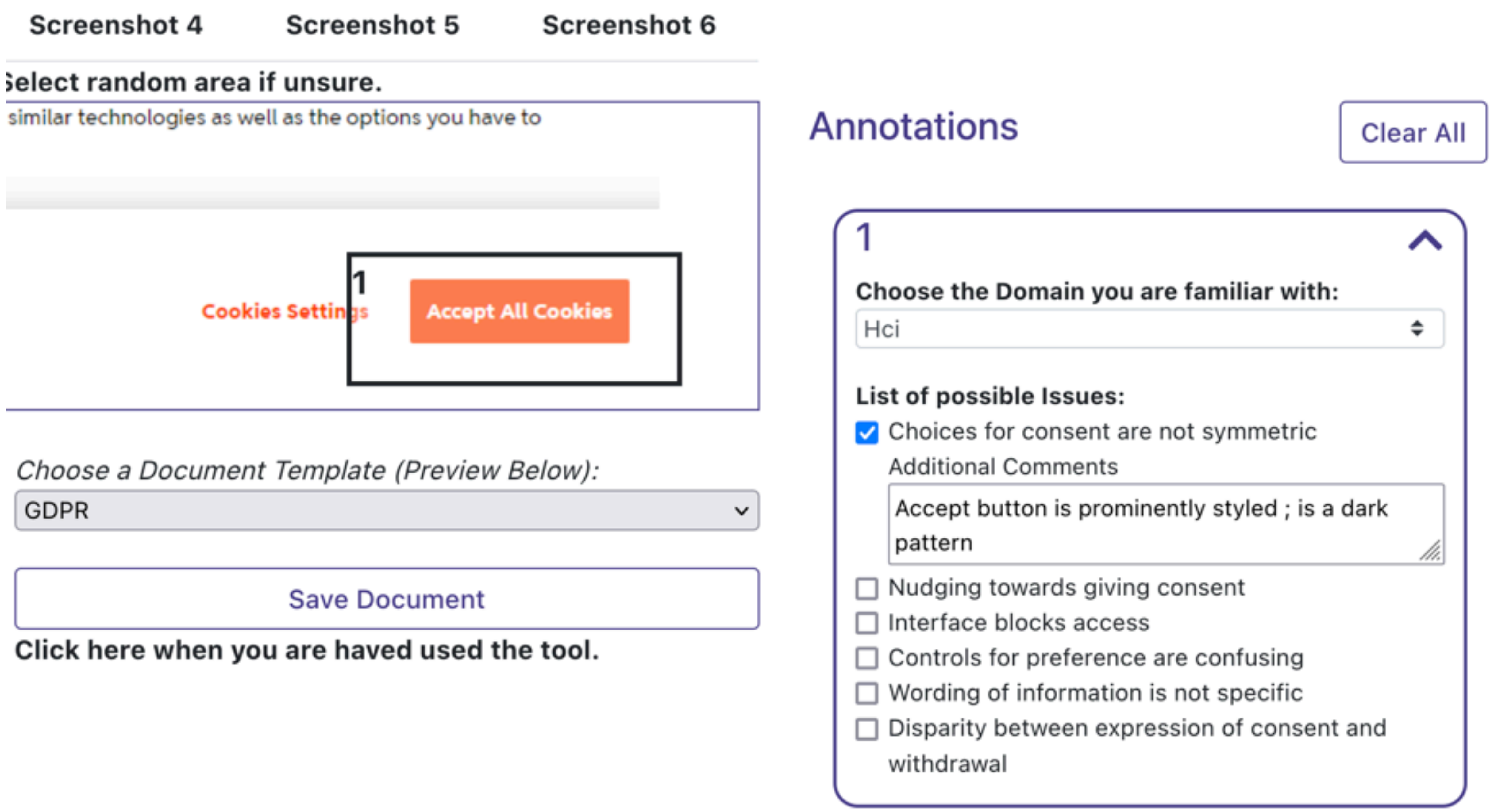
1.1.2 Information you choose to give us

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

How to Complaint Better?

Making it easier to report, investigate, document, and resolve issues online

https://brianlunch.github.io/ConsentAnnotationToolSite/#/study/



Select random area if unsure.

similar technologies as well as the options you have to

Choose a Document Template (Preview Below):

GDPR

Click here when you are haved used the tool.

Choose the Domain you are familiar with:

Hci

List of possible Issues:

☑ Choices for consent are not symmetric

Additional Comments

Accept button is prominently styled ; is a dark pattern

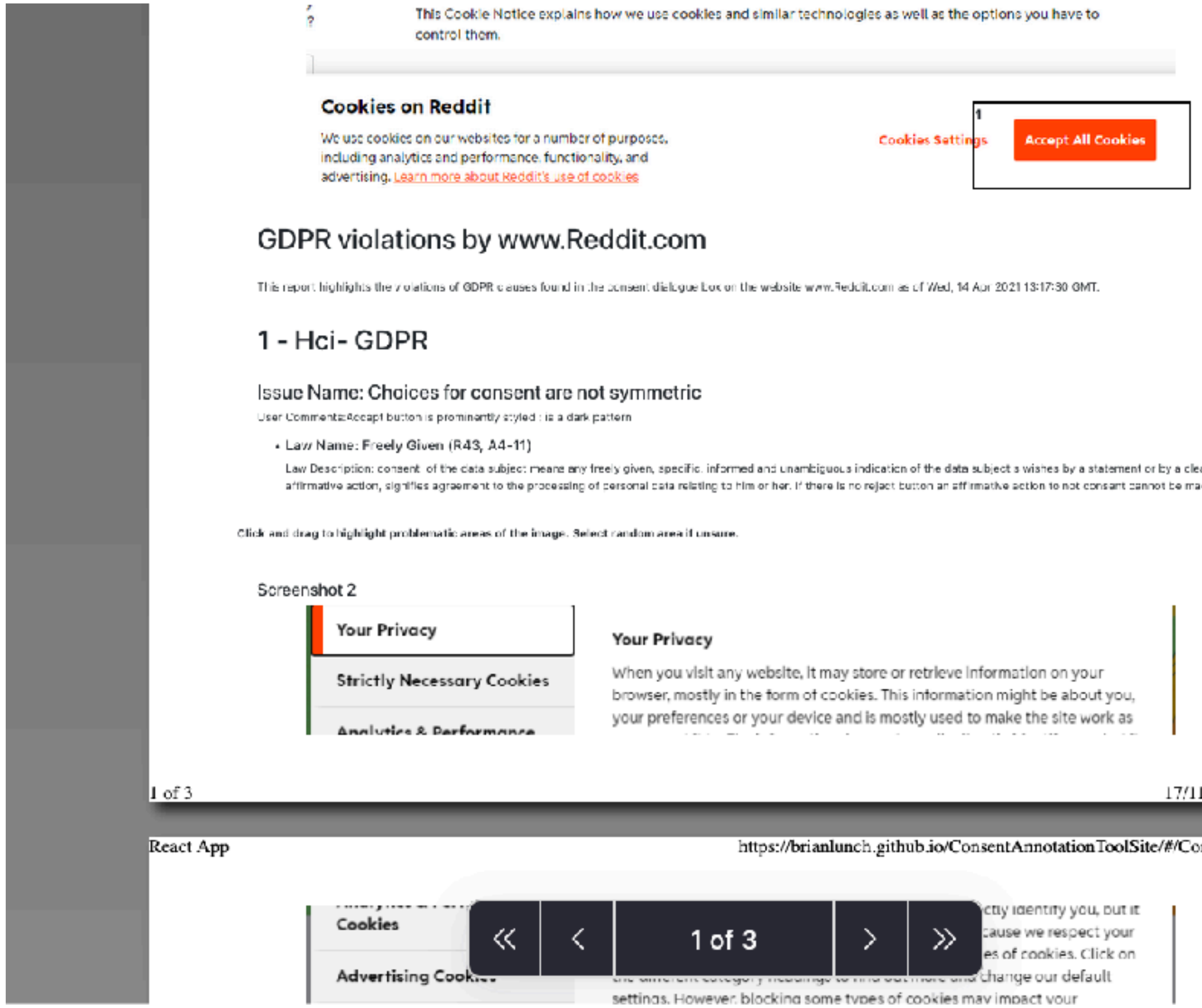
☐ Nudging towards giving consent

☐ Interface blocks access

☐ Controls for preference are confusing

☐ Wording of information is not specific

☐ Disparity between expression of consent and withdrawal



This Cookie Notice explains how we use cookies and similar technologies as well as the options you have to control them.

Cookies on Reddit

We use cookies on our websites for a number of purposes, including analytics and performance, functionality, and advertising. Learn more about Reddit's use of cookies

GDPR violations by www.Reddit.com

This report highlights the violations of GDPR clauses found in the consent dialogue box on the website www.Reddit.com as of Wed, 14 Apr 2021 13:17:30 GMT.

1 - Hci- GDPR

Issue Name: Choices for consent are not symmetric

User Comments:Accept button is prominently styled ; is a dark pattern

- Law Name: Freely Given (R43, A4-11)

  Law Description: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a cle affirmative action, signifies agreement to the processing of personal data relating to him or her. If there is no reject button an affirmative action to not consent cannot be ma

Click and drag to highlight problematic areas of the image. Select random area if unsure.

Screenshot 2

Your Privacy

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as

1 of 3

17/11

React App

https://brianlunch.github.io/ConsentAnnotationToolSite/#/Co

ctly identify you, but it
cause we respect your
es of cookies. Click on
change our default
settings. However, blocking some types of cookies may impact your

GDPR

Regulating Processing of Personal Data

Harshvardhan J. Pandit

pandith@tcd.ie | @coolharsh55

Regulating Big Tech - Utrecht Uni. | 20 December 2021 | Online/Virtual

Slides available at: https://harshp.com/research/presentations