Exercise 02:
GDPR, De-Identification, Privacy-Paradox

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

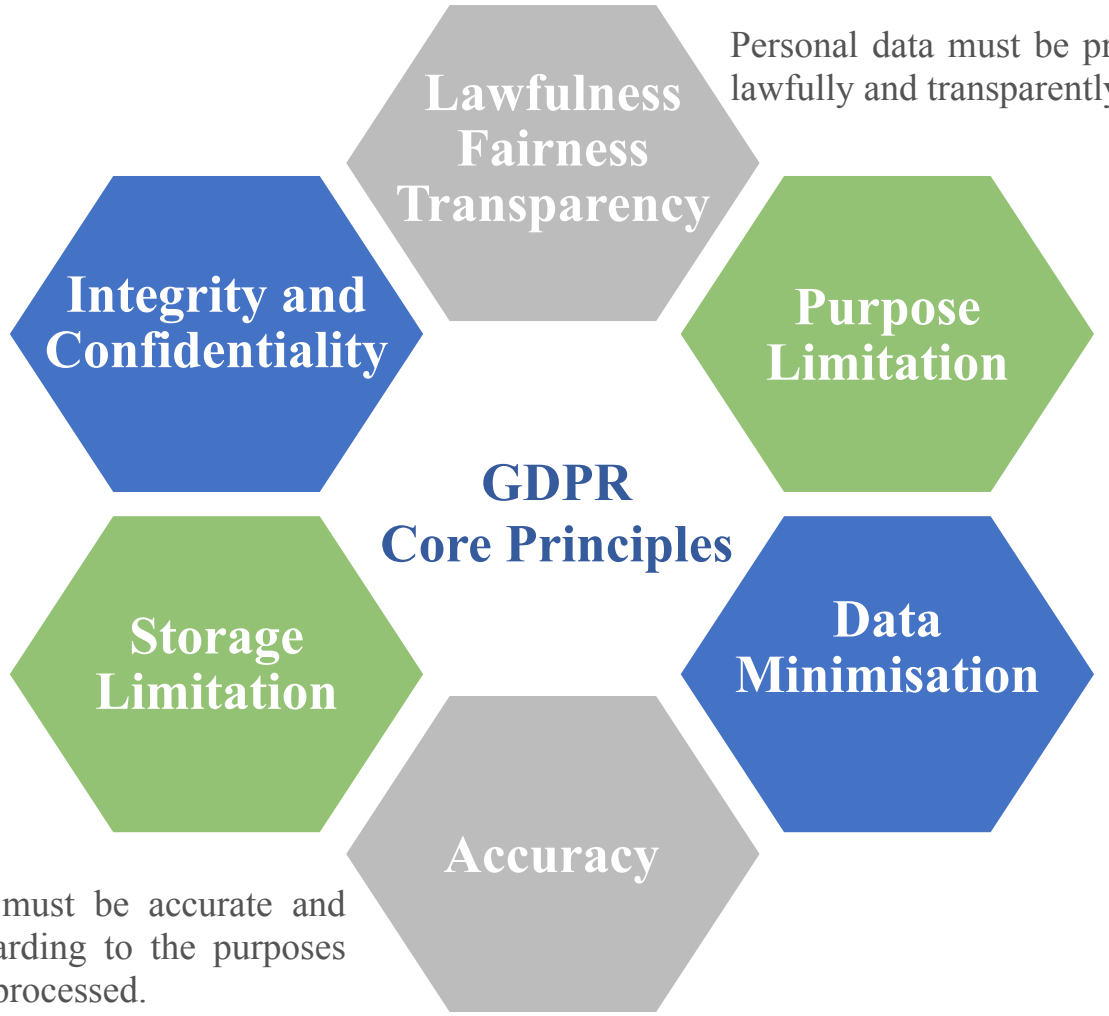
Task 1:

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

GDPR - Core Principles



Personal data must be processed in a lawfully and transparently.

Specific purposes for processing the data are mandatory and must be mentioned to the individuals.

Only the collection of personal data that is necessary to fulfil the purpose.

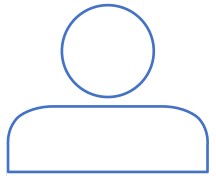
Personal data must be accurate and up-to-date regarding to the purposes for which it is processed.

Personal data must not be stored for no longer than necessary for the purpose.

Technical and organisational safeguards ensuring the security of the personal data are necessary.

GDPR - Legal Entity/Person vs. Natural Person

Legal Entity/Person



Natural Person

- Refers to an entity which is recognised by the law as having a legal personality, e.g., companies, corporations, natural persons, public institutions, etc.
- Can own property, enter contracts, pays taxes

- Identifiable natural person is one who can be identified **directly or indirectly**
- Identification via a reference to an identifier, e.g. name, id number, etc.
- Can own property, enter contracts, pays taxes, vote

GDPR - More terms …

Data Subject

The source of the (personal) data, e.g. a Natural Person

Personal Data

Any information relating to an identified or identifiable natural person

Controller

Responsible for processing (personal) data, e.g. a Legal Entity

Processing

Refers to any operation performed on personal data.

Consent

Consent regarding to privacy is a user decision, which must be given freely, specific, informed, and unambiguous.

GDPR - Types of Personal Data (1/2)

INTERNAL

Knowledge and Belief
Information about what a person knows or believes
religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks

Authenticating
Information used to authenticate an individual with something they know
passwords, PIN, mother's maiden name

Preference
Information about an individual's preferences or interests
opinions, intentions, interests, favorite foods, colors, likes, dislikes, music

HISTORICAL

Life History
Information about an individual's personal history
events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)

FINANCIAL

Account
Information that identifies an individual's financial account
credit card number, bank account

Ownership
Information about things an individual has owned, rented, borrowed, possessed
cars, houses, apartments, personal possessions

Transactional
Information about an individual's purchasing, spending or income
purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits

Credit
Information about an individual's reputation with regards to money
credit records, credit worthiness, credit standing, credit capacity

Source: https://enterprivacy.com

GDPR - Types of Personal Data (2/2)

EXTERNAL

Identifying
Information that uniquely or semi-uniquely identifies a specific individual
name, user-name, unique identifier, government issued identification, picture, biometric data

Ethnicity
Information that describes an individual's origins and lineage
race, national or ethnic origin, languages spoken, dialects, accents

Sexual
Information that describes an individual's sexual life
gender identity, preferences, proclivities, fetishes, history, etc.

Behavioral
Information that describes an individual's behavior or activity, on-line or off
browsing behavior, call logs, links clicked, demeanor, attitude

Demographic
Information that describes an individual's characteristics shared with others
age ranges, physical traits, income brackets, geographic

Medical and Health
Information that describes an individual's health, medical conditions or health care
physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions

Physical Characteristic
Information that describes an individual's physical characteristics
height, weight, age, hair color, skin tone, tattoos, gender, piercings

TRACKING

Contact
Information that provides a mechanism for contacting an individual
email address, physical address, telephone number

Location
Information about an individual's location
country, GPS coordinates, room number

Computer Device
Information about a device that an individual uses for personal use (even part-time or with others)
IP address, Mac address, browser fingerprint.

SOCIAL

Professional
Information about an individual's educational or professional career
job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions

Criminal
Information about an individual's criminal activity
convictions, charges, pardons

Public Life
Information about an individual's public life
character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data

Family
Information about an individual's family and relationships
amily structure, siblings, offspring, marriages, divorces, relationships

Social Network
Information about an individual's friends or social connections
friends, connections, acquaintances, associations, group membership

Communication
Information communicated from or to an individual
telephone recordings, voice mail, email

Source: https://enterprivacy.com

GDPR - Frequently used Terms

Accountability
This is the first step in achieving data compliance; you need to understand and designate who in your business owns data.

Natural Person
In legal terms, a natural person is a person that is an individual human being.

Legal Person
A legal Person, in contrast to a natural person, is an individual, company, or other entity which has legal rights.

Data Subject
The source of the (personal) data.

Personal Data
A person's data (name, id number, location data, physiological, genetic, mental.)

Data Processor
The organisation that processes personal data on behalf of the Data Controller.

Data Controller
The organisation that collects and uses Personal Data. The Data Controller is a person who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

Processing
Anything you do to the personal data is classed as processing. This includes, but not limited to: recording, structuring, storing and analysis.

Consent
Unambiguous indication, or clear positive action individual gives (via verbal agreement, or expressed in writing) signifying they agree with the processing of their personal Data. Consent can also be called 'Permissions'.

Profiling
When you process data with the aim of making an informed decision about an individual. Namely to analyse their preferences, interests, behaviour, location or movements.

Right to be informed
The Data Subject's right to receive adequate and clear information about how their data is, will, or could be used. This could be an open and transparent privacy policy.

Legitimate interests
A very grey area. The right a company has for contacting an individual based on their judgement that the individual will legitimately want (or need) to receive the information.

PII
Any bit of information (data) that allows you to identify an individual person.

DPO
The individual or legal entity with the responsibility to advise and inform the Data Processor of their obligations under GDPR.

DPIA
The way to identify any risks in the methods used to process data.

Data Breach
This is what the GDPR aims to prevent when the security of an individual's Personal Data is compromised and exposed.

Right to erasure
The Data Subject's right to request that they are erased from your database.

Right to restrict processing
The Data Subject's right to prevent the processing of personal data. This does not mean you have to delete it, but you cannot do more than store it.

PII: Personally Identifiable Information DPO: Data Protection Officer DPIA: Data Protection Impact Assessment

Source: https://www.i-scoop.eu/gdpr/

Task 2:
De-Identification

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

Anonymization

Anonymization is a useful tool, because the principles of data protection should apply to any information concerning an identified or identifiable natural person.

→ No data protection must be applied to anonymous (personal) data

Anonymous Data:

- information which does not relate to an identified or identifiable natural person
- personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

How to determine whether a natural person is identifiable?

- **All reasonable means** likely to be used to identify the natural person **directly or indirectly**
- "Reasonable Means" according to objective factors:
  - Costs and amount of time required for identification
  - Available technology at the time
  - Technological developments

Pseudonymization

- Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information
- Additional information can be kept separately and secured
- Especially useful in environments, where the Data Subject needs to be re-identificated like the Health Care Domain

Name	Age	Hobby
Max Mustermann	26	Football
Alice Wonderland	23	Photography

Identification via Name

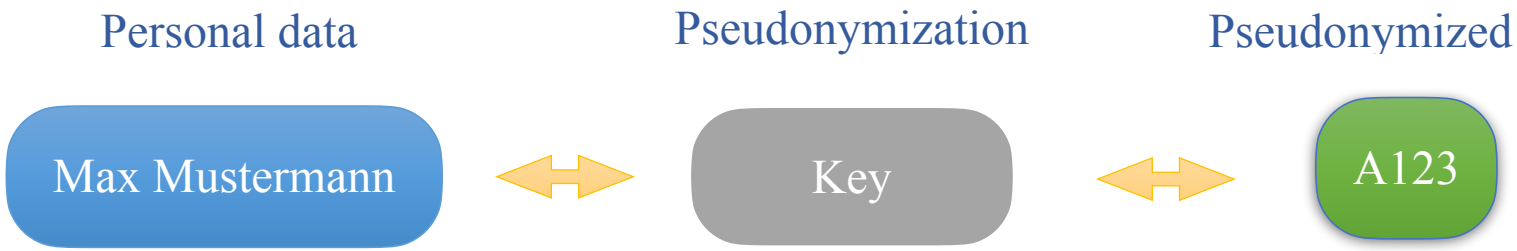
Name	Age	Hobby
A123	26	Football
B234	23	Photography

Name	Pseudonym
Max Mustermann	A123
Alice Wonderland	B234

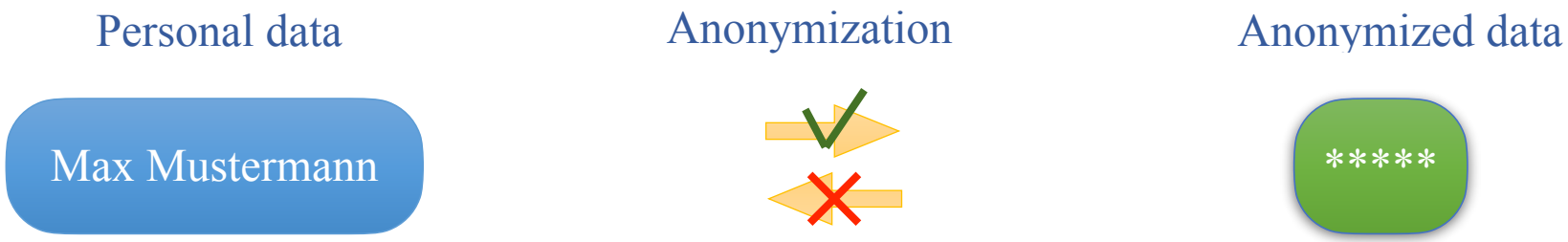
Additional Information, e.g.,
protected by encryption

Anonymization vs. Pseudonymization

Pseudonymisation



Anonymisation

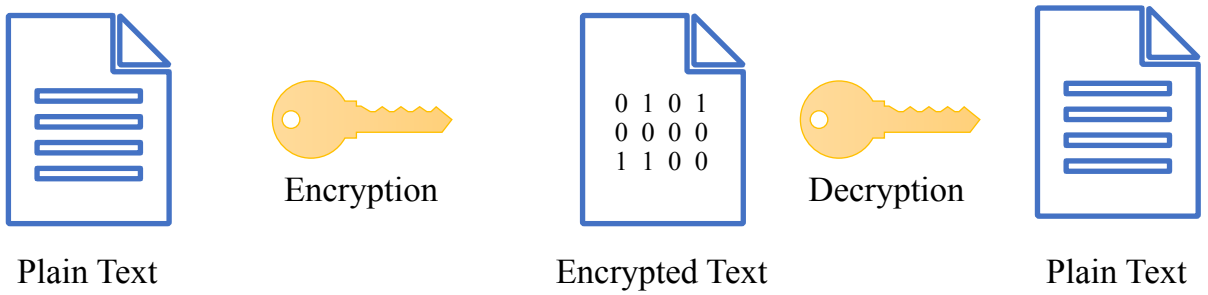


Source: https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/

Encryption

Converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key.

- Bidirectional encryption: Encryption & Decryption are possible
- Symmetric encryption: Same key for Encryption & Decryption
- Asymmetric encryption: Public and private keys for Encryption & Decryption



Source: https://aboutssl.org/hashing-vs-encryption/

Hashing

- "One-way" encryption = hashing
- Usually relatively fast
- Uses random values
- Does not support Decryption (Exception: Trapdoor hash functions)

Source: https://aboutssl.org/hashing-vs-encryption/

→ Encryption and Hashing are useful tools which are exploited in some Anonymization and Pseudonymization methods.

Task 3:
Privacy-Paradox

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

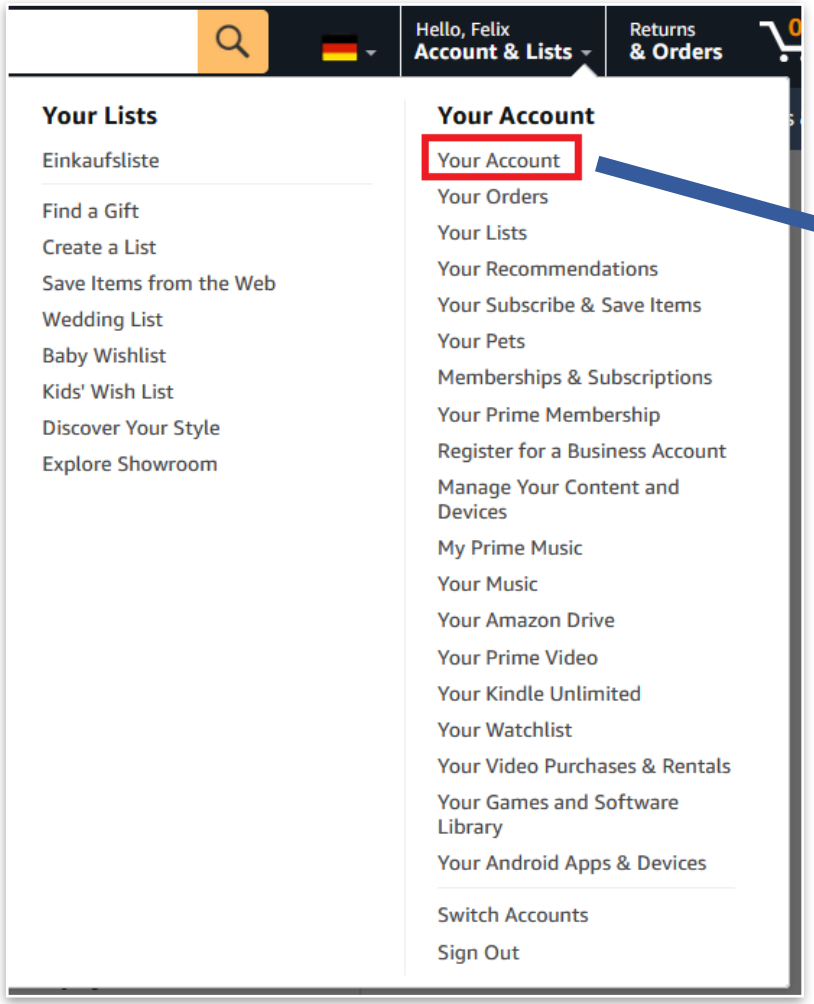
GDPR - Privacy Paradox

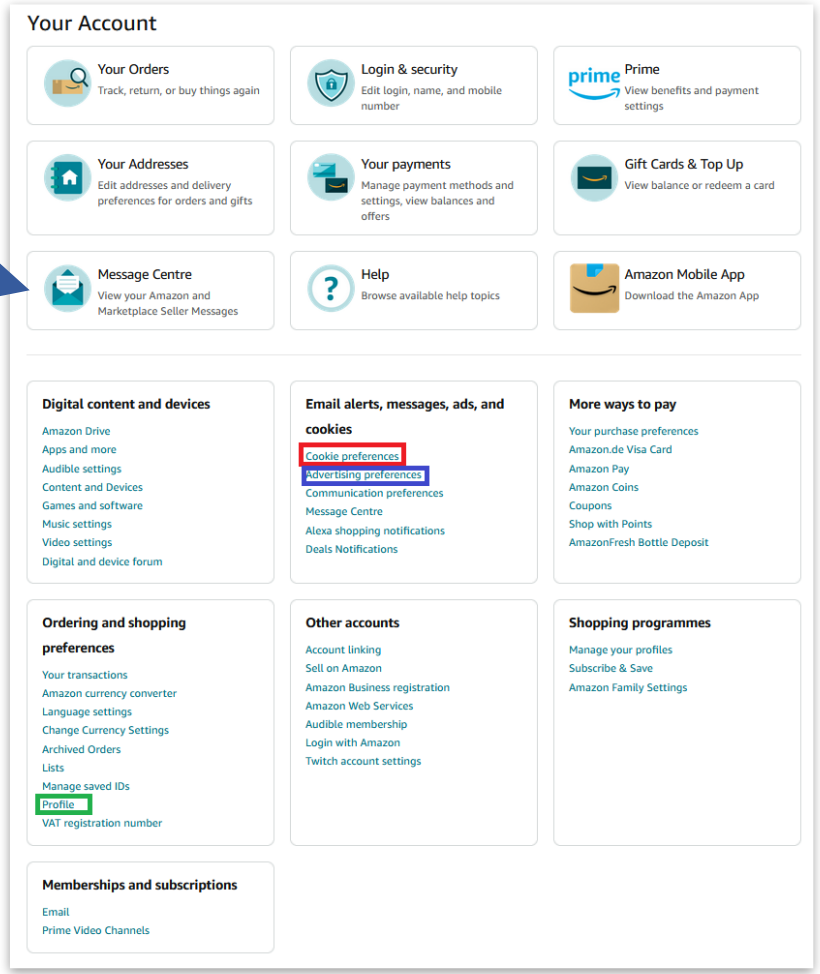
- Privacy is highly important for most Data Subjects
- In most cases, the effort to protect its Personal Data outweighs the benefit

How to support a Data Subject?

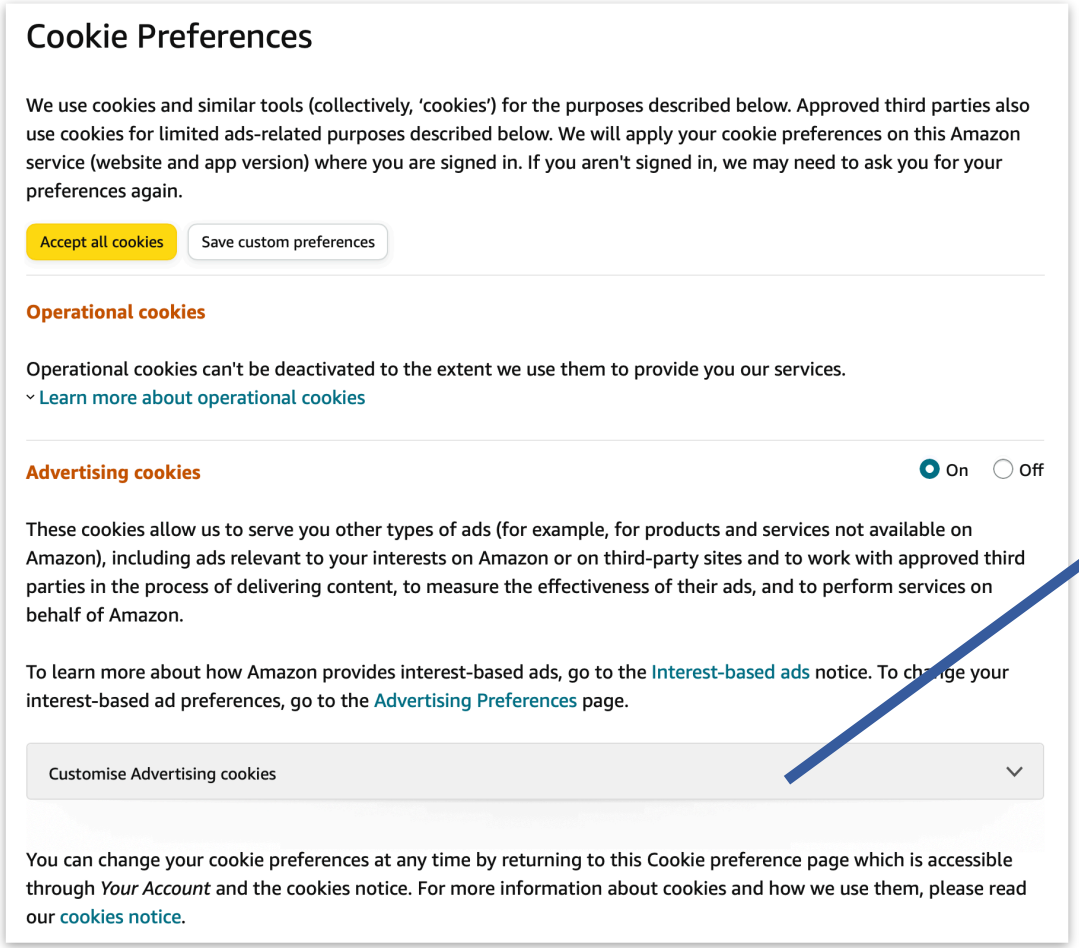
→ Design minimalistic and easy-to-use privacy enforcing UIs

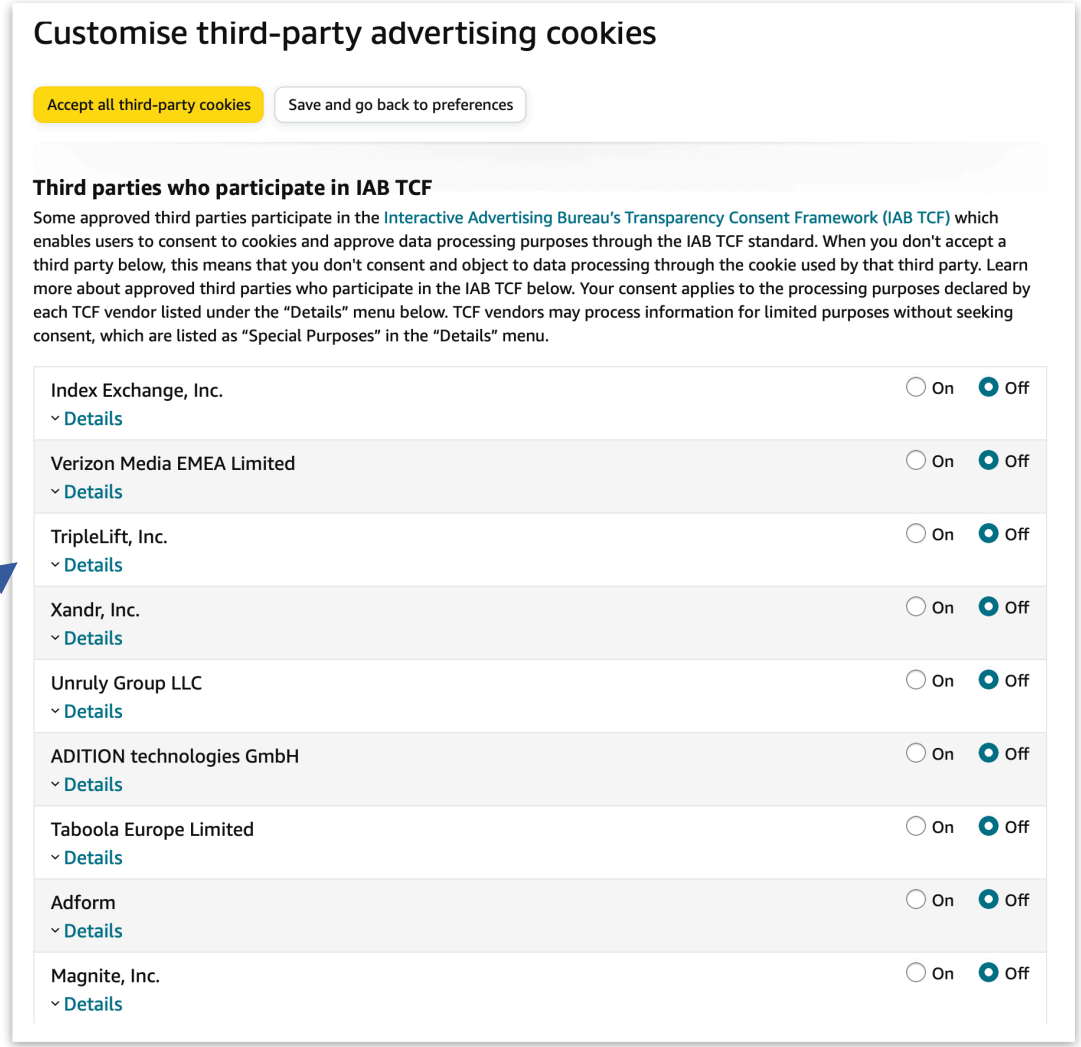
Discussion - Amazon: An Unexpected Journey 1



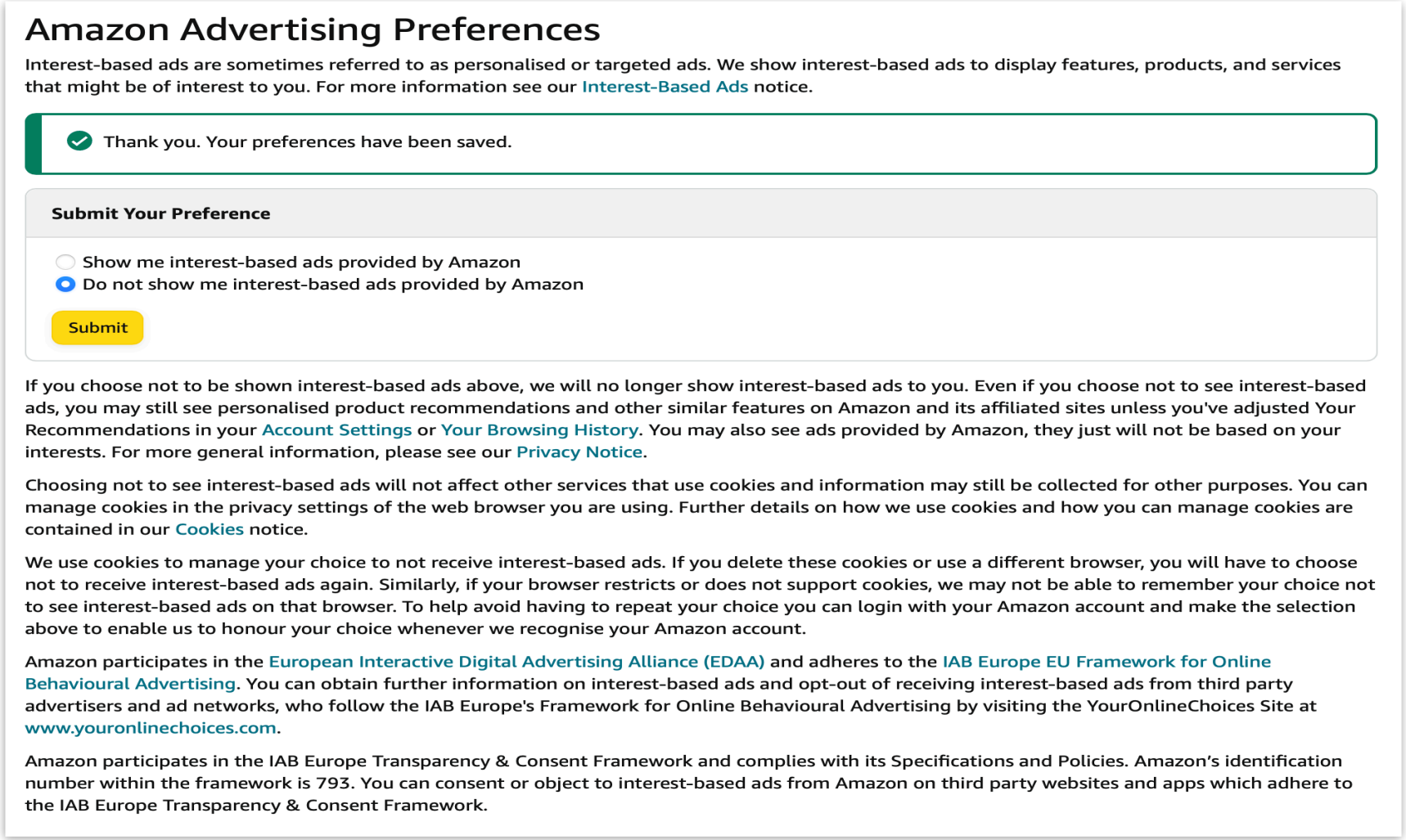


Discussion - Amazon: An Unexpected Journey 2





Discussion - Amazon: An Unexpected Journey 3



Amazon Advertising Preferences

Interest-based ads are sometimes referred to as personalised or targeted ads. We show interest-based ads to display features, products, and services that might be of interest to you. For more information see our Interest-Based Ads notice.

Thank you. Your preferences have been saved.

Submit Your Preference

- ○ Show me interest-based ads provided by Amazon
- ◉ Do not show me interest-based ads provided by Amazon

Submit

If you choose not to be shown interest-based ads above, we will no longer show interest-based ads to you. Even if you choose not to see interest-based ads, you may still see personalised product recommendations and other similar features on Amazon and its affiliated sites unless you've adjusted Your Recommendations in your Account Settings or Your Browsing History. You may also see ads provided by Amazon, they just will not be based on your interests. For more general information, please see our Privacy Notice.

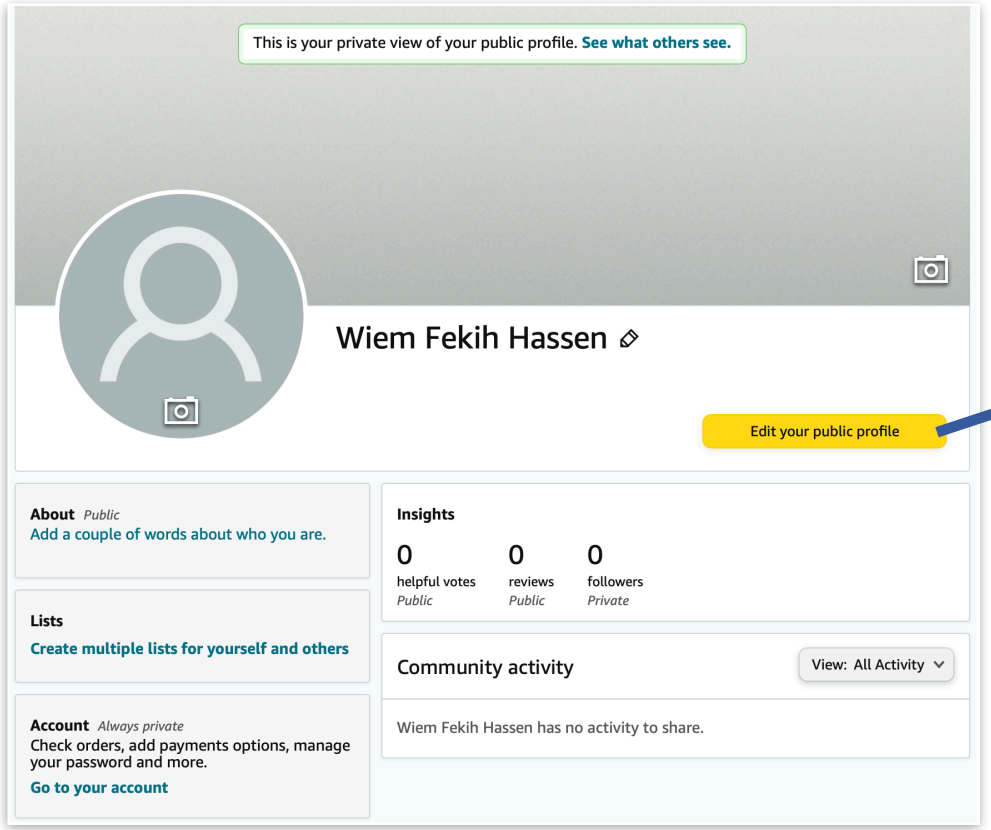
Choosing not to see interest-based ads will not affect other services that use cookies and information may still be collected for other purposes. You can manage cookies in the privacy settings of the web browser you are using. Further details on how we use cookies and how you can manage cookies are contained in our Cookies notice.

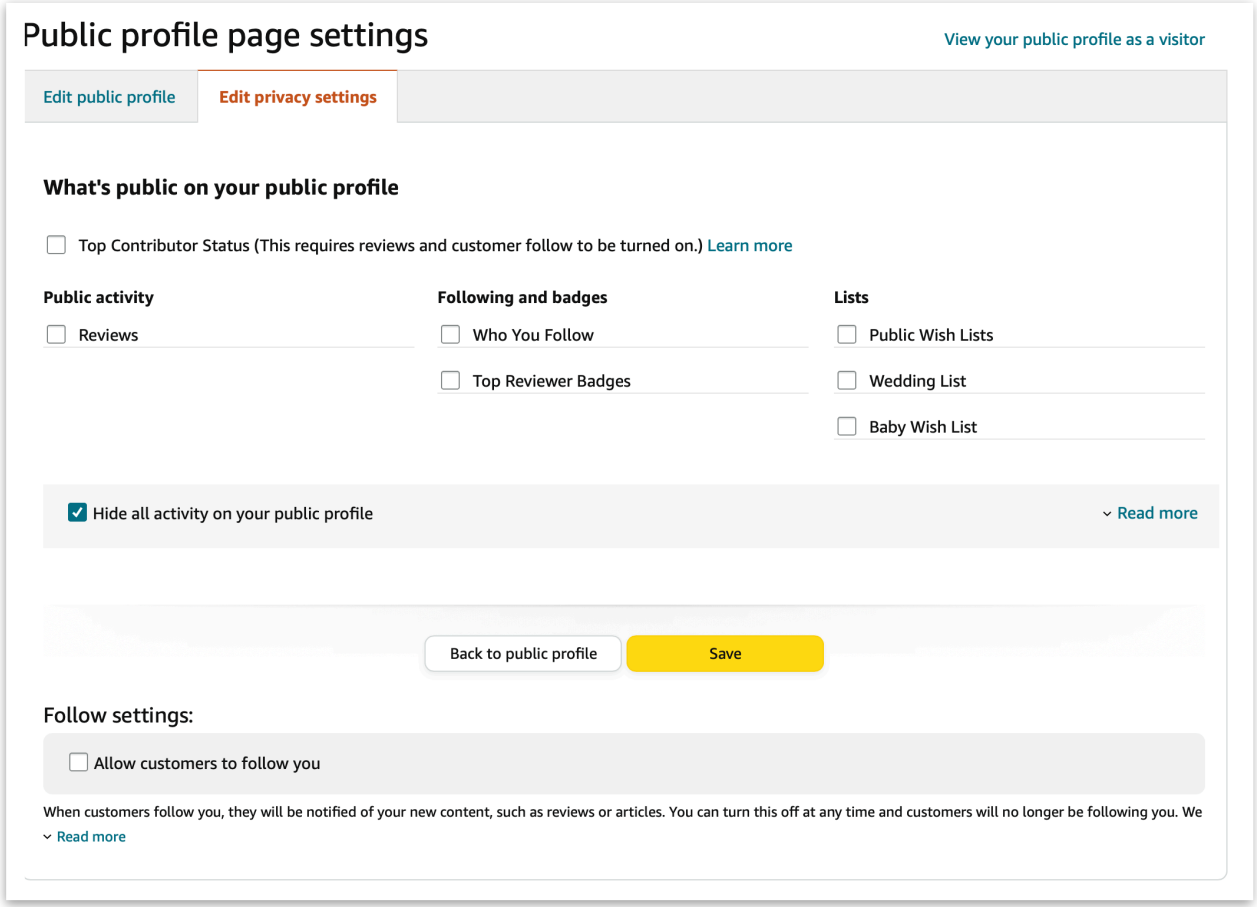
We use cookies to manage your choice to not receive interest-based ads. If you delete these cookies or use a different browser, you will have to choose not to receive interest-based ads again. Similarly, if your browser restricts or does not support cookies, we may not be able to remember your choice not to see interest-based ads on that browser. To help avoid having to repeat your choice you can login with your Amazon account and make the selection above to enable us to honour your choice whenever we recognise your Amazon account.

Amazon participates in the European Interactive Digital Advertising Alliance (EDAA) and adheres to the IAB Europe EU Framework for Online Behavioural Advertising. You can obtain further information on interest-based ads and opt-out of receiving interest-based ads from third party advertisers and ad networks, who follow the IAB Europe's Framework for Online Behavioural Advertising by visiting the YourOnlineChoices Site at www.youronlinechoices.com.

Amazon participates in the IAB Europe Transparency & Consent Framework and complies with its Specifications and Policies. Amazon's identification number within the framework is 793. You can consent or object to interest-based ads from Amazon on third party websites and apps which adhere to the IAB Europe Transparency & Consent Framework.

Discussion - Amazon: An Unexpected Journey 4

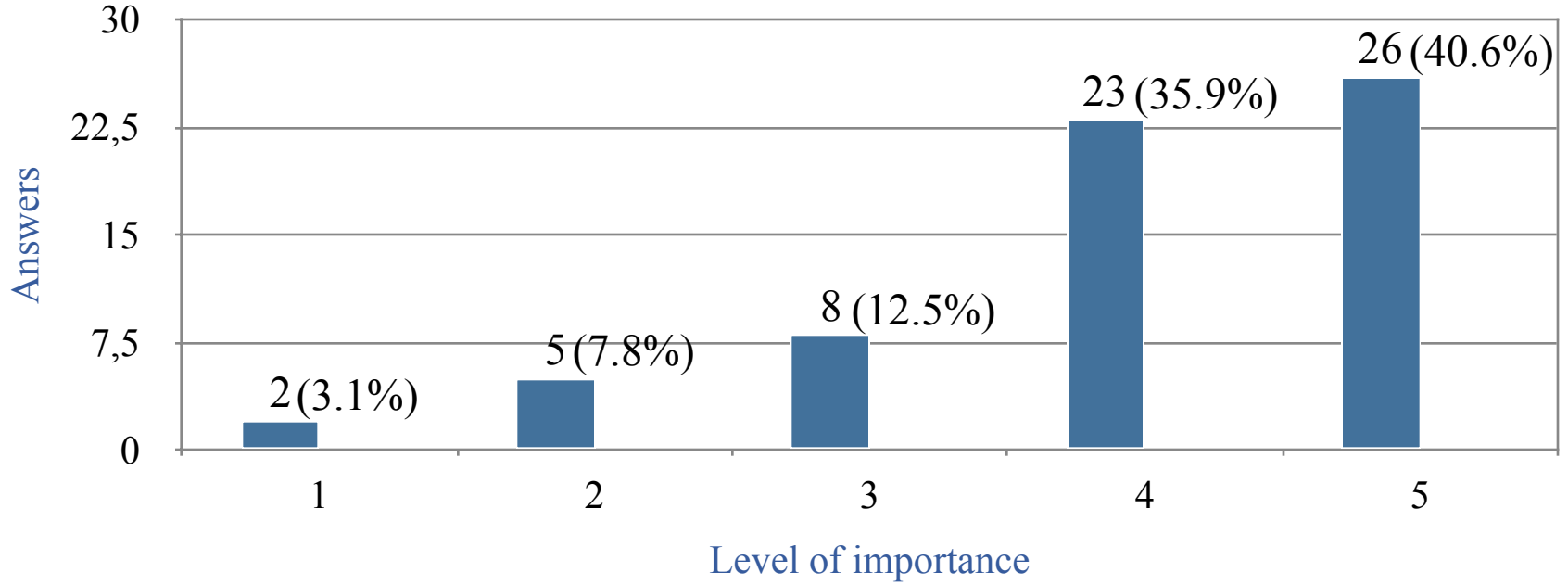




Privacy Paradox - Our Small Survey (Q1)

Q1: How important do you value your personal privacy on the internet?

64 Answers



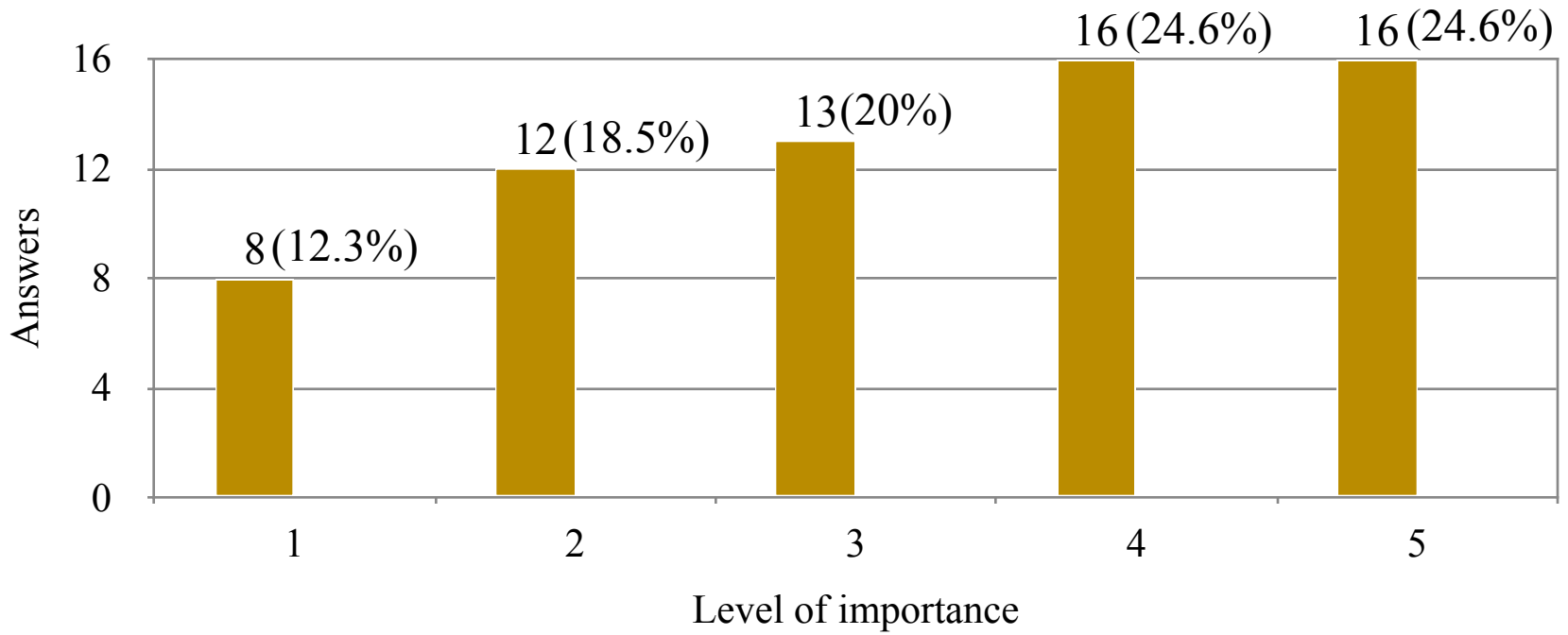
1: Not at all

5: Highly

Privacy Paradox - Our Small Survey (Q2)

Q2: How often do you accept all cookies offered by visited websites?

65 Answers



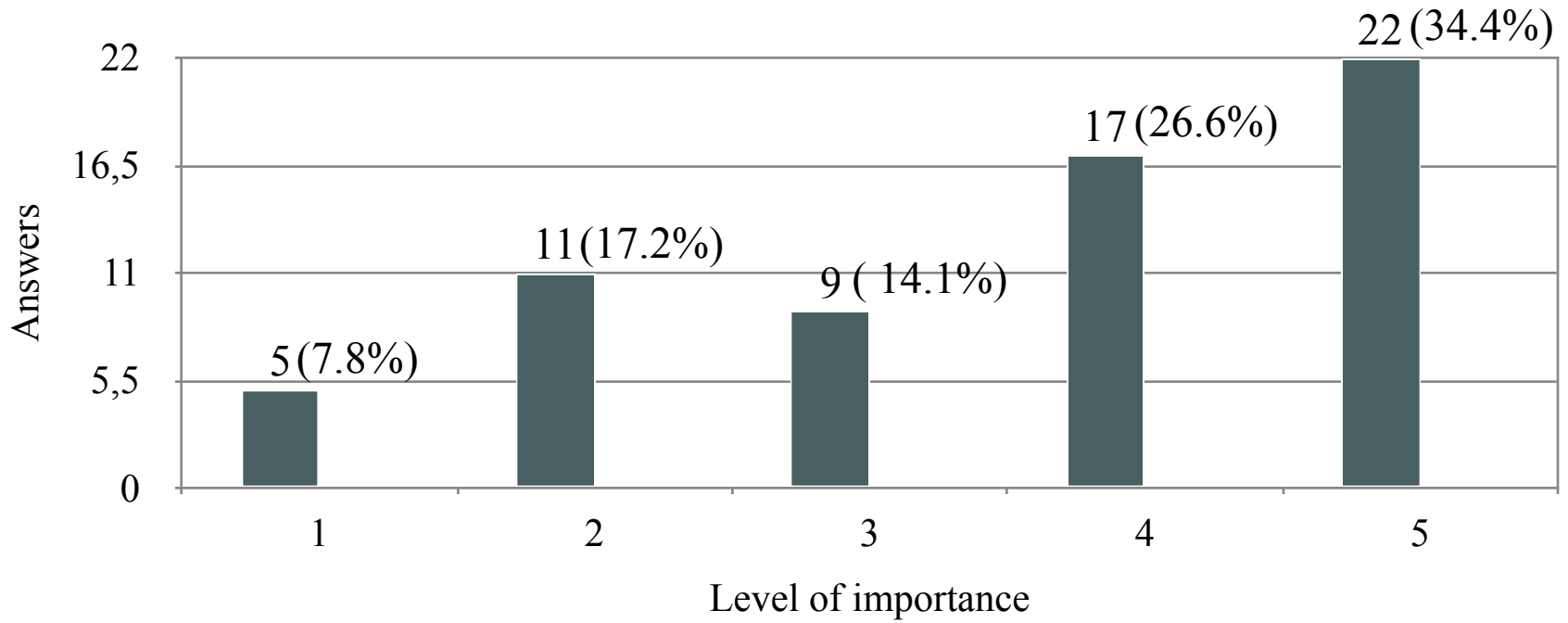
1: Not at all

5: Highly/Frequently

Privacy Paradox - Our Small Survey (Q3)

Q3: How often do you only accept the necessary cookies offered by visited websites?

64 Answers



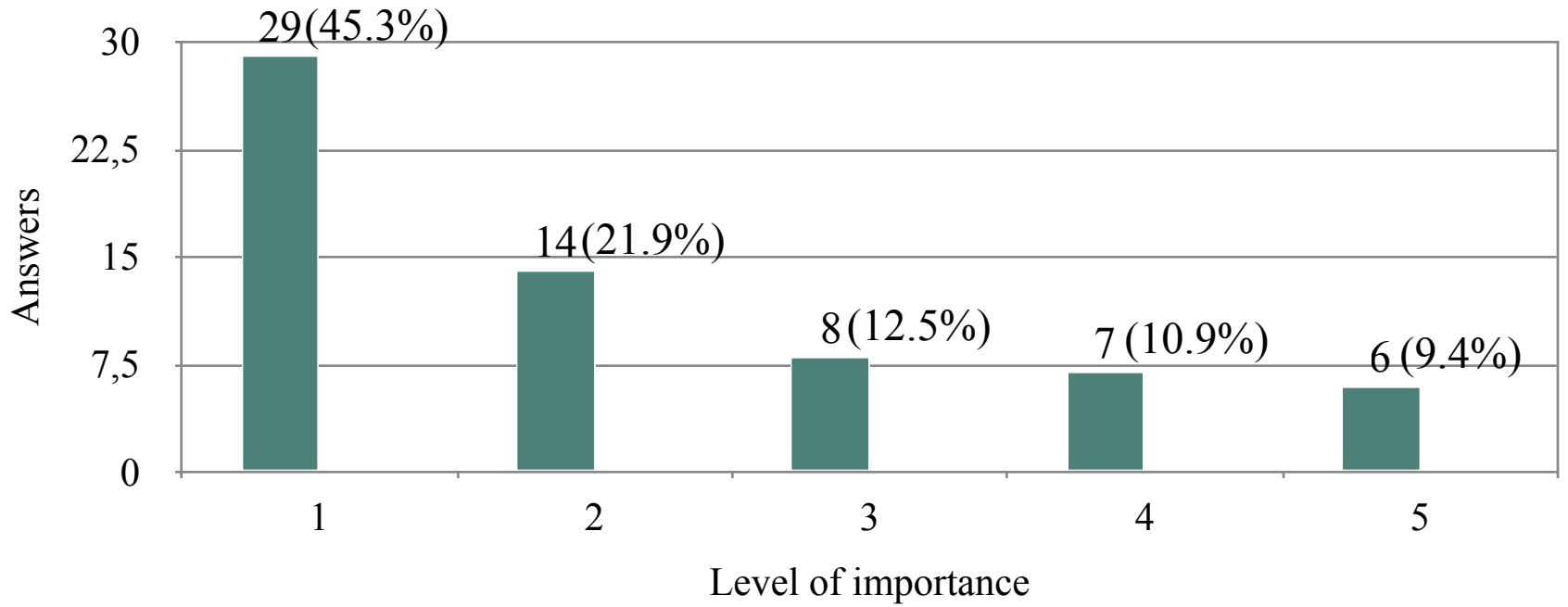
1: Not at all

5: Highly/Frequently

Privacy Paradox - Our Small Survey (Q4)

Q4: How often do you only manually customize cookies offered by visited websites?

64 Answers



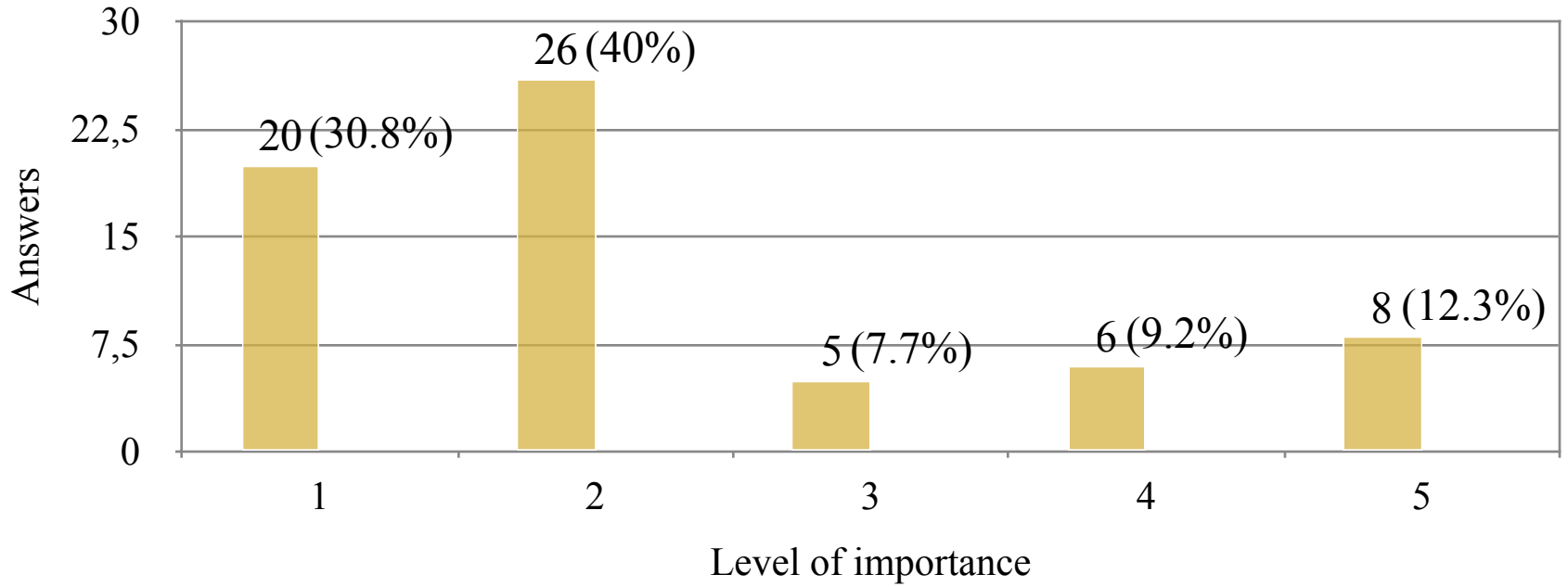
1: Not at all

5: Highly/Frequently

Privacy Paradox - Our Small Survey (Q5)

Q5: How often have you manually customized your privacy settings on a website with that functionality, e.g. Amazon (cookies are not meant here)?

65 Answers



1: Not at all

5: Highly/Frequently

Privacy Paradox - Our Small Survey (Q6)

Q6: Have you ever customized your privacy settings on the Operating System (OS) of your computer or phone?

64 Answers

See you next week ☺