JÖNKÖPING UNIVERSITY

Web development and privacy

GDPR and the e-privacy directive

2020-09-14

PART 1 – INTRODUCTION TO GDPR

The General Data Protection Regulation exists to protect individuals' fundamental rights and freedoms, in particular their right to protection of their personal data.

INTRODUCTION - FILMS

WHAT IS GDPR?

- New EU legislation - **G**eneral **D**ata **P**rotection **R**egulation
- GDPR is a legal framework for the collection and processing of personal information from individuals who live in the European Union (EU).
- The Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.
- The Regulation also applies to all processing of personal data by an organization within the EU.

GDPR IS INTENDED TO

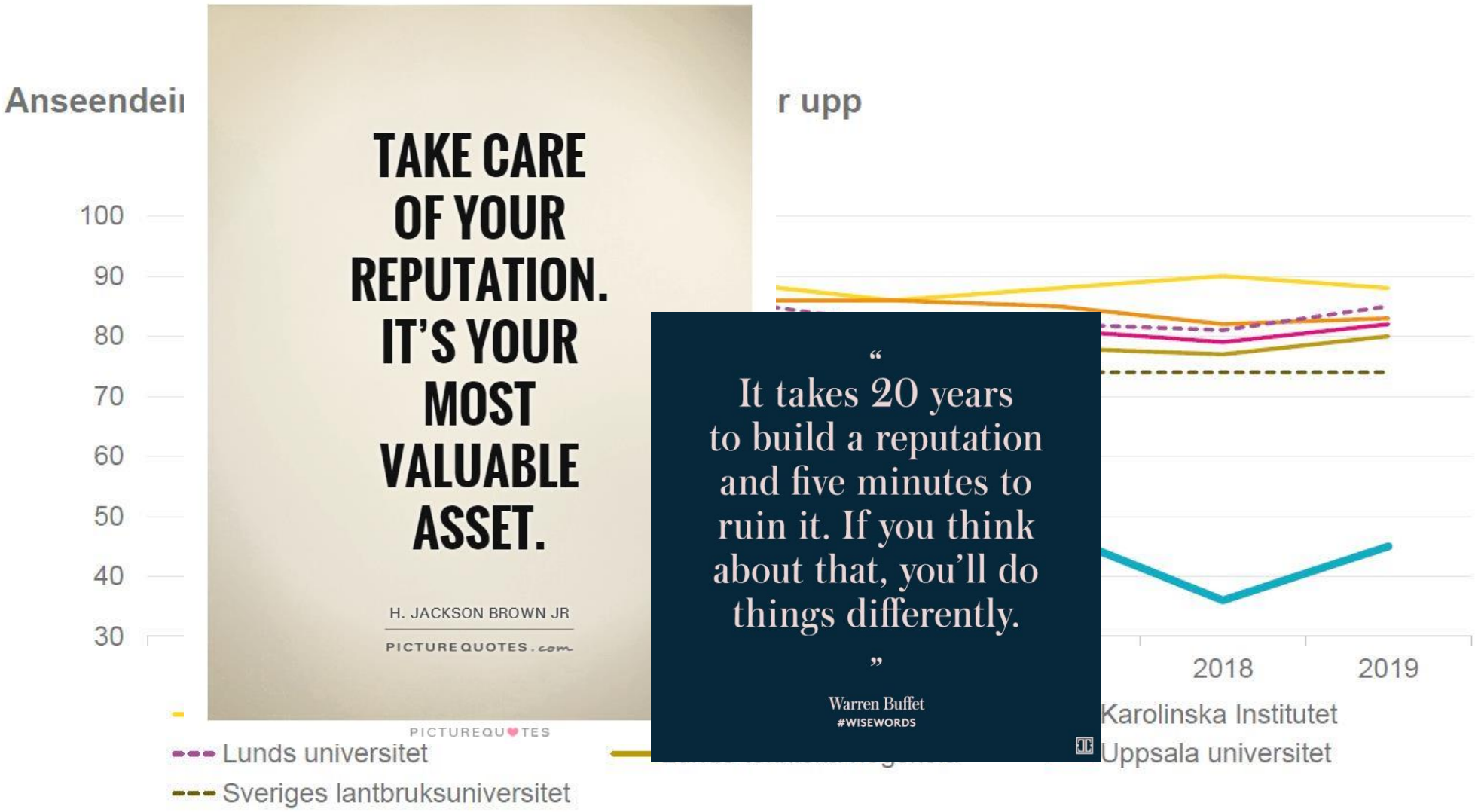
- Enforce the EU Convention on Human Rights
- Make citizens masters of their own personal data
- Strengthen and unify data protection for individuals within the European Union
- Unify and simplify the regulatory environment for international businesses

GDPR IS INTENDED TO

The General Data Protection Regulation (GDPR) applies throughout the European Union and its purpose is to create a uniform and harmonised level for the protection of personal data so that the free movement of personal data within Europe is not hindered.

GDPR - FINES AND PENALTIES

- https://www.enforcementtracker.com/


Anseendei
r upp
100
90
80
70
60
50
40
30
2018
2019
Karolinska Institutet
Uppsala universitet
Lunds universitet
Sveriges lantbruksuniversitet
TAKE CARE OF YOUR REPUTATION. IT'S YOUR MOST VALUABLE ASSET.
H. JACKSON BROWN JR
PICTUREQUOTES.com
PICTUREQUOTES
"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."
Warren Buffet
#WISEWORDS

WHAT IS PERSONAL DATA?

Any information that directly or indirectly can be attributed to a living person.

PERSONAL DATA

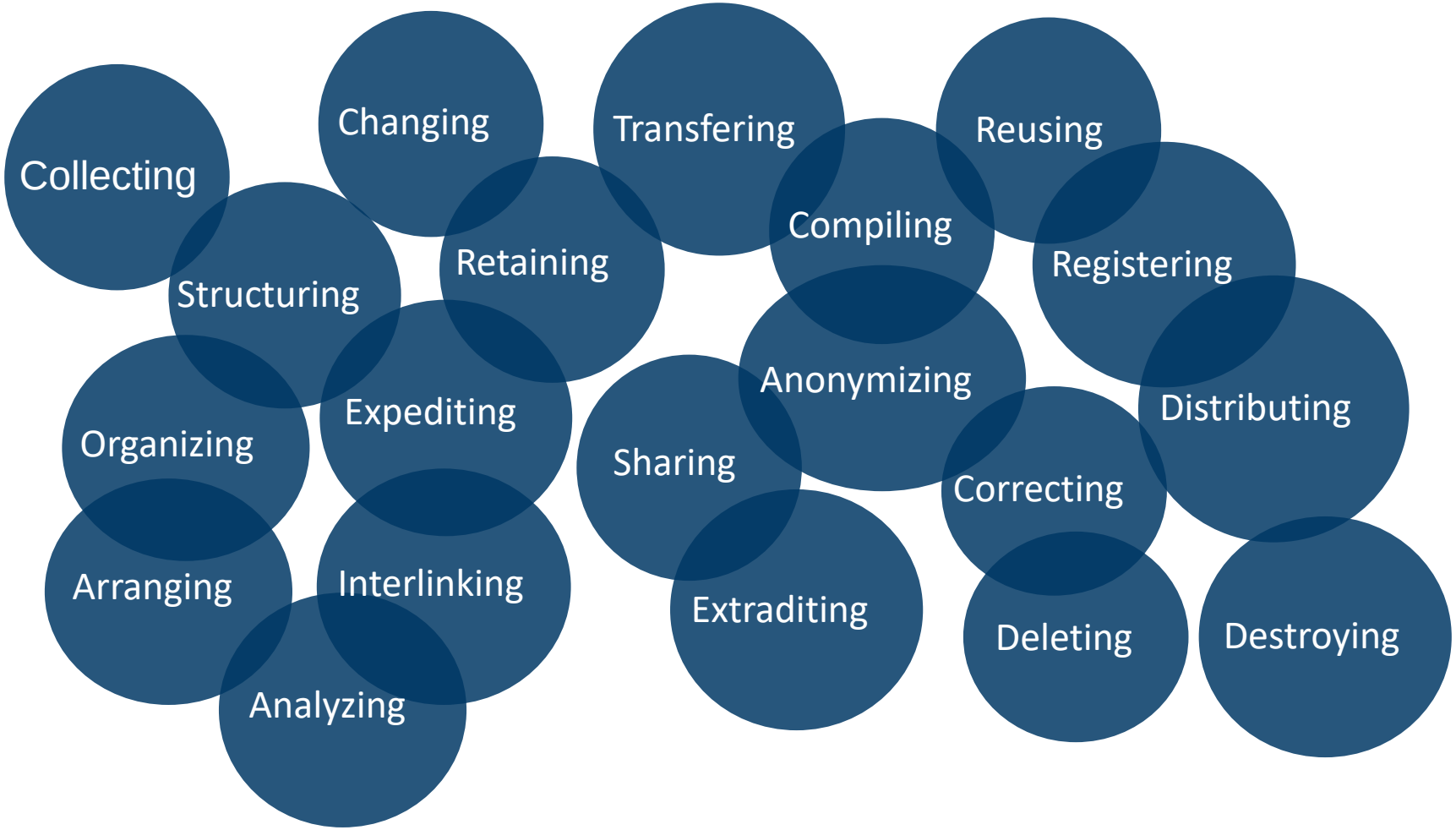
- Direct
- Indirect
- Objective
- Subjective
- Encrypted

Name, adress, postal code, social security number, car registration number, pictures, voice recordings, videos etc.

SENSITIVE PERSONAL DATA:

- **race or ethnic origin**
- **political opinions**
- **religious or philosophical beliefs**
- **trade-union membership**
- **health or sex life and sexual orientation**
- **genetic or biometric data**

PROCESSING PERSONAL DATA



DEFINITIONS OF KEY ROLES

DATA SUBJECT

- An identified or identifiable natural person.

CONTROLLER

- A natural or legal person, public authority, agency or other body that determines the purposes and means of the processing of personal data.

PROCESSOR

- A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

DATA PROCESSING - PRINCIPLES

- Purpose limitation - Determined, specific, explicit and limited
- Lawfulness - Lawful basis
- Minimization - In context of relevance and purpose
- Accuracy - Data is correct and up to date
- Information - Duty to inform data subjects
- Protection - Reduce risks based on risk assessment
- Retention - Accomplish purpose, then delete personal data

LAWFUL BASIS FOR PROCESSING

- Legal obligation
- Necessary to exercise public authority
- **Contractual necessity**
- Protection of vital interests
- Public interest
- **Legitimate interest**

  or
- **Consent**

CONSIDERATIONS

Factors to consider when processing personal data:

- Purpose: Why is personal data processing needed?
- Legality: Is the purpose lawful? What is the lawful basis?
- Minimize: What data is needed for my purpose and for how long?
- Security: How do I reduce or eliminate risks?

PART 2 - E-PRIVACY DIRECTIVE

INTRODUCTION - FILMS

THE E-PRIVACY DIRECTIVE (EPD)

- A specialized EU-regulation focused on protecting privacy and security of personal data in electronic communications
  - ePD is focused on communications
  - ePD covers more than personal data, specifically web cookies and traffic data

- A new e-Privacy Directive is in the works.

THE E-PRIVACY DIREKTIVE AND COOKIES

- In Sweden: the Electronic Communications Act - Lag (2003:389) om elektronisk kommunikation

”6 kap 18 § Data may be stored in or retrieved from a subscriber's or user's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and consents to it. This does not prevent such storage or access as is necessary for the transmission of an electronic message via an electronic communications network or which is necessary to provide a service expressly requested by the user or subscriber.”

PRECEDENT – EU COURT

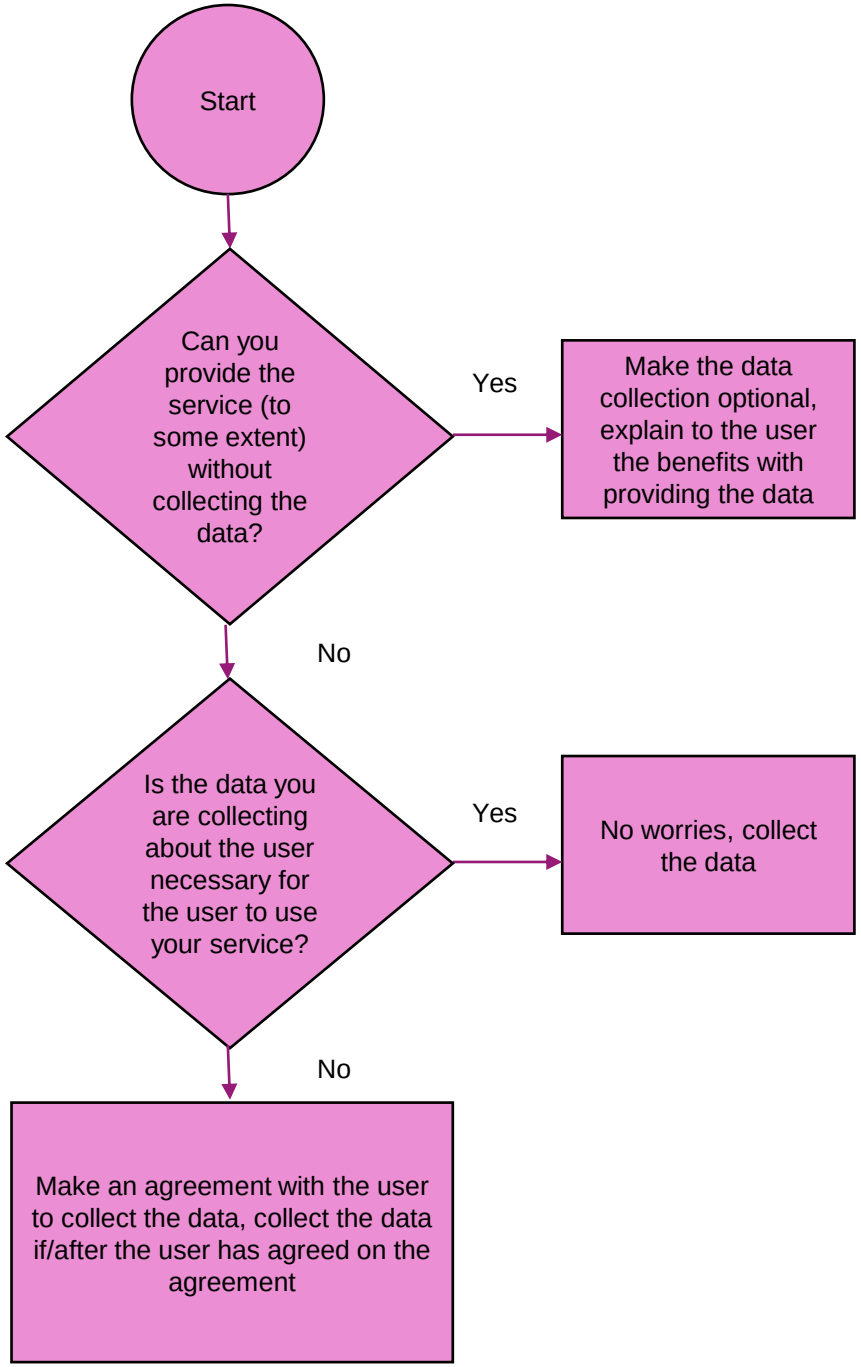
- The European Court of Justice states that the use of cookies requires the active consent of website visitors (ruling in case C-673/17, 1-10-2019).
- A box checked in advance is not enough.
- The ruling means that most websites must review how they obtain website visitors' consent for cookies used for analytics tools, marketing, advertising networks and other purposes.

CONSENT IN GDPR

- The legal basis of consent means that the data subject has agreed to the processing of personal data
- Consent must be voluntary and equal
- Voluntary means that data subjects have a genuinely free choice and control over their personal data
- The data subject must not suffer negative consequences if he does not give his consent, e.g. denied access to or access to content on a web page

CHECKLIST - WEB DEVELOPMENT

- ❑ Is personal data processing necessary?
- ❑ Define a specific and defined purpose
- ❑ Decide appropriate security measures (Storage, encryption, etc.)
- ❑ Set data retention period
- ❑ Register data processing in a GDPR-register
- ❑ Manage lawful basis and information to data subjects
- ❑ Collect and process data (Cookies, customer data etc.)
- ❑ Delete data according to set data retention period


Start
Can you provide the service (to some extent) without collecting the data?
Yes
Make the data collection optional, explain to the user the benefits with providing the data
No
Is the data you are collecting about the user necessary for the user to use your service?
Yes
No worries, collect the data
No
Make an agreement with the user to collect the data, collect the data if/after the user has agreed on the agreement

COOKIES – THE GOOD, THE BAD AND THE UGLY

Examples of personal data processing - Web

- The good: https://www.datainspektionen.se/
- The bad and ugly: https://www.mirror.co.uk/

- Factors:
  - Purpose
  - Information to data subjects
  - Legal basis
  - Minimization

RESOURCES

- www.datainspektionen.se
  - Data Protection Agency (DPA) for Sweden - Issues directives and codes of statutes. The DPA also handles complaints and carries out inspections.
- https://dataskydd.net/
  - Dataskydd.net is a private non-profit organization working on making data protection easier.
- https://webbkoll.dataskydd.net/sv/
  - A web-based test tool that finds out how good the data protection is on a website, and gives tips on how to fix the problems that the test tool finds

JÖNKÖPING UNIVERSITY

QA OM COOKIES

- - Måste en användare godkänna användandet av alla olika sorters kakor (temporära/sessionsknutna, långlivade, etc.)?
  - Får man använda kakor innan användaren har godkänt/nekat användande av kakor?
  - Vad behövs för att få en användares godkännande att använda kakor?
  - Hur styrker man att en användare har givit sitt godkännande?
  - Vad för risker finns det med att använda kakor utan att användaren godkänner det?
  - Är det OK att vägra användaren åtkomst till sidan om denne inte accepterar kakor?
  - Vad behöver man tänka på om användare kan skapa konton och logga in på ens hemsida (då personuppgifter sparas)?
  - Om användare kan skicka in något anonymt (t.ex. gästboksinlägg), påverkas det av GDPR på något vis? Även om det inte kan knytas till en specifik individ?