CT255
Introduction to Cybersecurity

Lecture 1

GDPR

Dr. Michael Schukat, 2019-22

Motivation

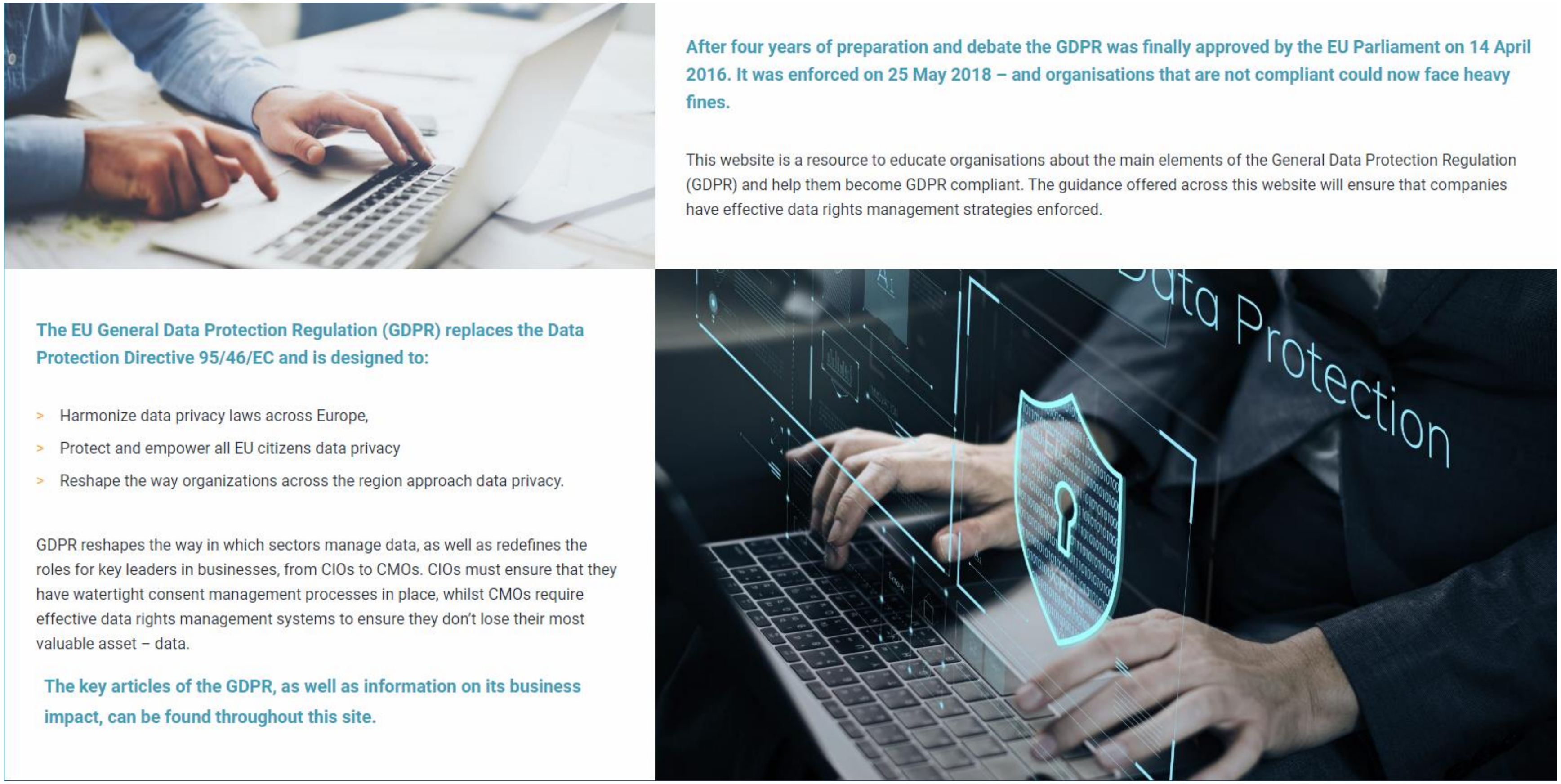
- Cyberattacks are aimed at **accessing, changing, or destroying sensitive information**, extorting money, or interrupting normal business processes
- So managing sensitive data may reduce the attack probability or at least its impact
- GDPR provides such a regulatory framework

General Data Protection Regulation

- GDPR is a binding regulation in EU law on data protection in the EU and the European Economic Area (EEA), that became enforceable on 25 May 2018
- It also addresses the transfer of personal data outside the EU and EEA areas
- The GDPR's primary aim is to **enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business**
- The regulation **contains provisions and requirements related to the processing of personal data of individuals** who are located in the EEA, and applies to any enterprise—**regardless of its location and the data subjects' citizenship or residence**—that is processing the personal information of individuals inside the EEA

Mx2

GDPR Summary: https://www.gdpreu.org/



After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. It was enforced on 25 May 2018 – and organisations that are not compliant could now face heavy fines.

This website is a resource to educate organisations about the main elements of the General Data Protection Regulation (GDPR) and help them become GDPR compliant. The guidance offered across this website will ensure that companies have effective data rights management strategies enforced.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to:

> Harmonize data privacy laws across Europe,
> Protect and empower all EU citizens data privacy
> Reshape the way organizations across the region approach data privacy.

GDPR reshapes the way in which sectors manage data, as well as redefines the roles for key leaders in businesses, from CIOs to CMOs. CIOs must ensure that they have watertight consent management processes in place, whilst CMOs require effective data rights management systems to ensure they don't lose their most valuable asset – data.

The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

What is Data Protection?

- Data protection is about an **individual's fundamental right for privacy**
- When an individual gives their personal data to any organisation, the recipient has the duty to keep the data safe and private
- Data protection legislation
  - governs the way we deal with personal data / information
  - provides a mechanism for safeguarding privacy rights of individuals in relation to the processing of their data
  - upholds rights and enforces obligations

Mx6

NUI Galway
OÉ Gaillimh

Personal Data

- 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"
- Applies to printed and electronic data

Sensitive Personal Data

- Racial origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic Data (e.g. biological samples)
- Biometric Data (e.g. fingerprints)
- Data concerning health
- Data concerning a person's sex life or sexual orientation
- **Explicit consent is required to process special categories of personal data**

HTTP Cookies

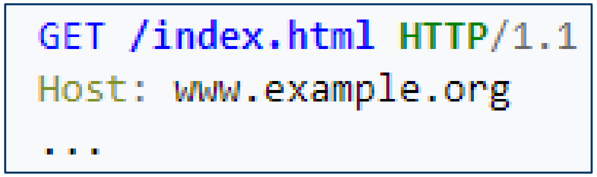
- An (HTTP) cookie is a small piece of data stored on the user's computer by the web browser while browsing a website
- Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity
- They can also be used to remember pieces of information that the user previously entered into form fields
- Authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with

Cookie Implementation

- Cookies are arbitrary pieces of data (i.e. large random strings), usually chosen and first sent by the web server, and stored on the client computer by the web browser
- The browser then sends them back to the server with every request
- Browsers are required to:
  - support cookies as large as 4,096 bytes in size
  - support at least 50 cookies per domain (i.e. per website)
  - support at least 3,000 cookies in total

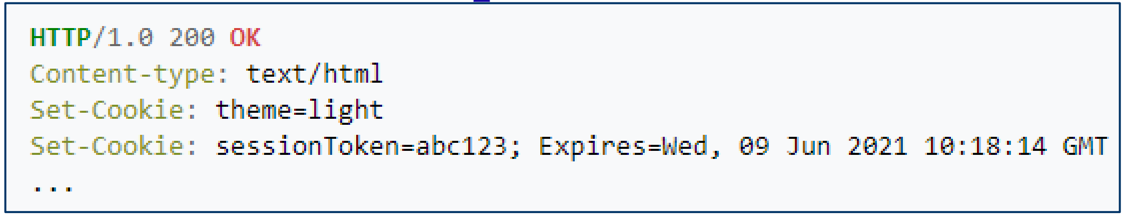
Setting a Cookie - Example

- A browser sends its first request for the homepage of www.example.org, resulting in the GET request



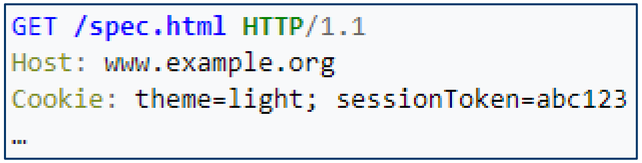
```
GET /index.html HTTP/1.1
Host: www.example.org
...
```

- The server responds with



```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT
...
```

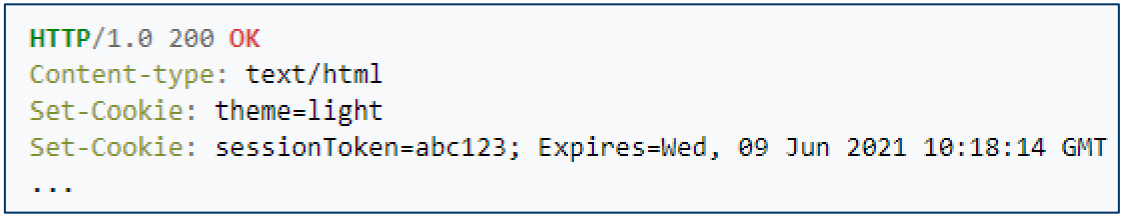
- Later client requests to this server will contain these cookies:



```
GET /spec.html HTTP/1.1
Host: www.example.org
Cookie: theme=light; sessionToken=abc123
…
```

Cookie Structure

- A cookie consists of the following components:
  - Name
  - Value
  - Zero or more attributes (name/value pairs) Attributes store information such as the cookie's expiration, domain, and flags (such as *Secure* and *HttpOnly*)



```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT
...
```

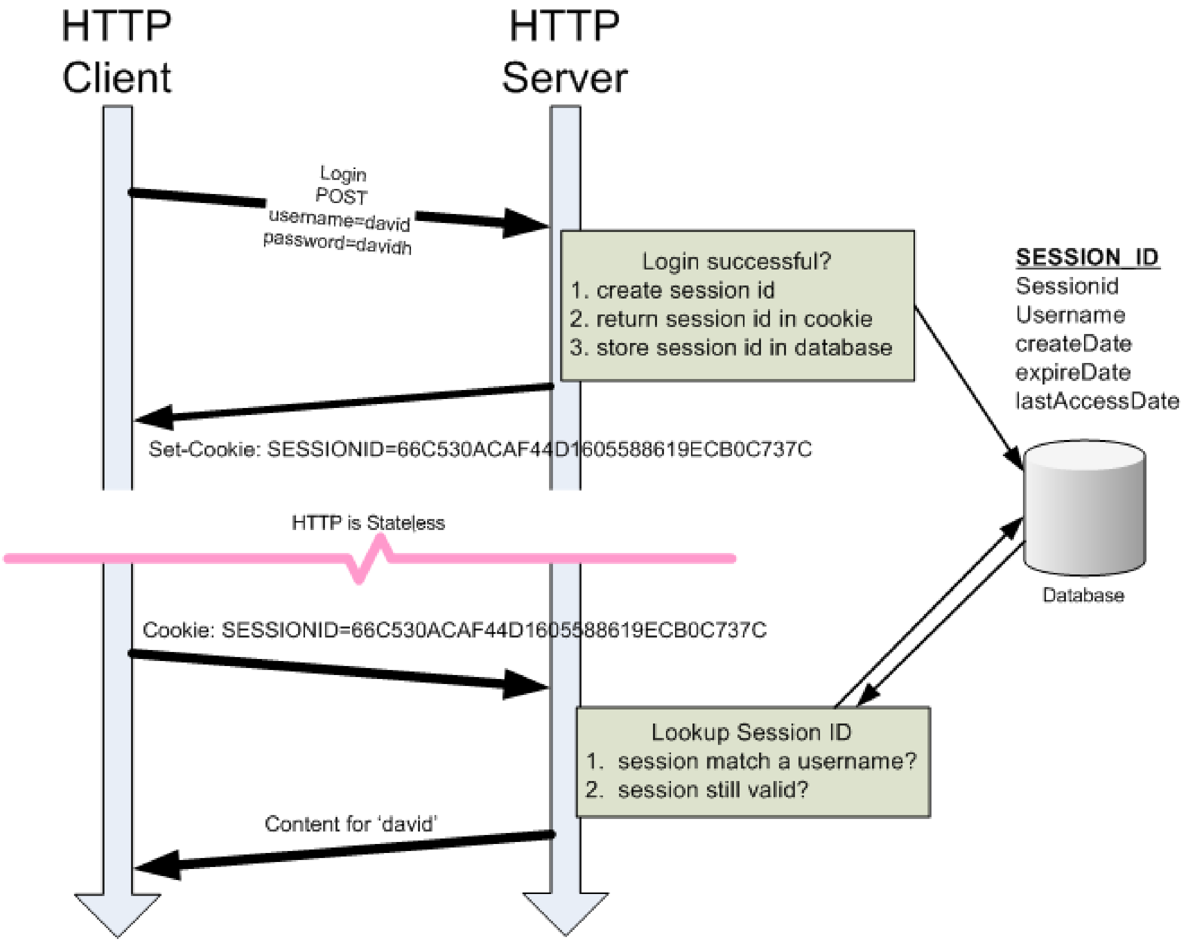
Session Cookies

- A session cookie (aka in-memory cookie, transient cookie or non-persistent cookie) exists only in temporary memory while the user navigates its website
- Web browsers normally delete session cookies when the user closes the browser
- Session cookies do not have an expiration date assigned to them, which is how the browser knows to treat them as session cookies
- Example: “theme” cookie on previous slide

Persistent Cookie

- A persistent cookie expires at a specific date or after a specific length of time
- For the persistent cookie's lifespan set by its creator, its information will be transmitted to the server every time the user visits the website that it belongs to
- … or every time the user views a resource belonging to that website from another website (such as an advertisement).
  For this reason, persistent cookies are sometimes referred to as tracking cookies because they can be used by advertisers to record information about a user's web browsing habits
- However, they are mainly used for legitimate reasons, such as keeping users logged into their accounts on websites, to avoid re-entering login credentials at every visit
- Example: “sessionToken” cookie in the previous example

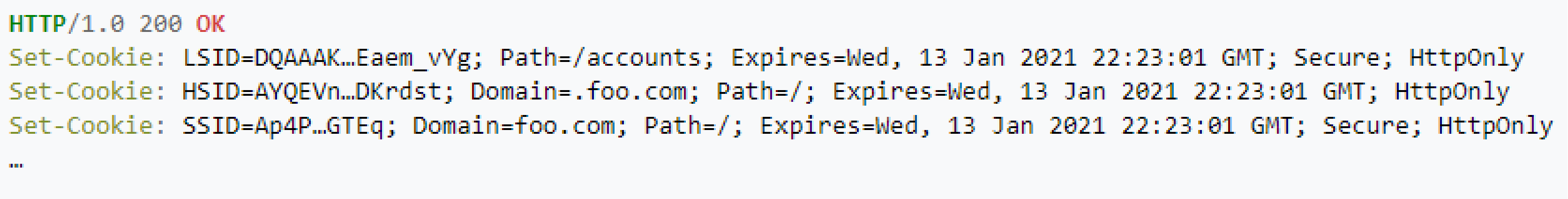
Session Management via Persistent Cookies



NUI Galway
OÉ Gaillimh

Cookie Attributes

- Consider the following response header sent by a webserver that contains 3 persistent cookies:

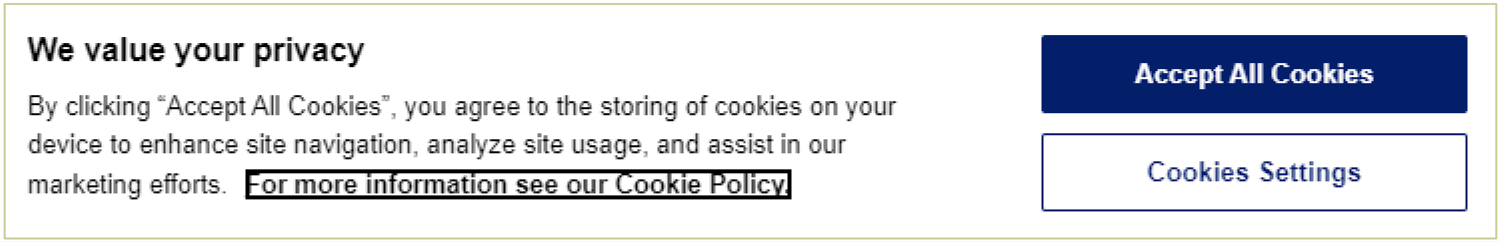


```
HTTP/1.0 200 OK
Set-Cookie: LSID=DQAAAK…Eaem_vYg; Path=/accounts; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
Set-Cookie: HSID=AYQEVn…DKrdst; Domain=.foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; HttpOnly
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
…
```

- The *Domain* and *Path* attributes define the cookie's scope
- The *Secure* attribute makes sure that the cookie can only be transmitted over an encrypted connection (i.e. HTTPS → later), making it a **secure cookie**
- The *HttpOnly* attribute directs browsers not to expose cookies through channels other than HTTP / HTTPS requests
  This means that this **HttpOnly cookie** cannot be accessed via client-side scripting languages (notably JavaScript)

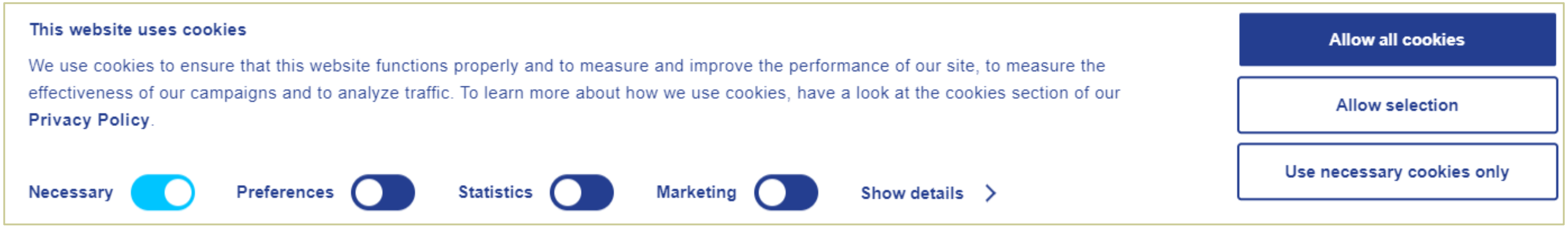
GDPR and Cookies

- Generally, a user’s consent must be sought before a cookie is installed in a web browser



We value your privacy

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. For more information see our Cookie Policy



This website uses cookies

We use cookies to ensure that this website functions properly and to measure and improve the performance of our site, to measure the effectiveness of our campaigns and to analyze traffic. To learn more about how we use cookies, have a look at the cookies section of our **Privacy Policy**.

Necessary ● Preferences ○ Statistics ○ Marketing ○

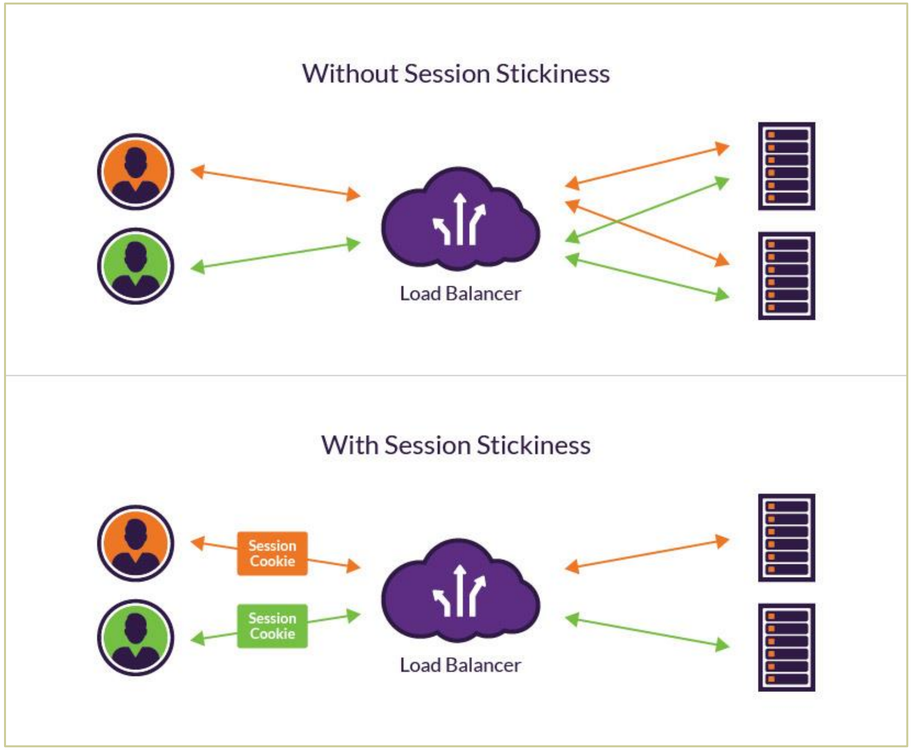
- There are two exemptions:
  - The communications exemption
  - The strictly necessary exemption

The *Communications Exemption*

- This applies to cookies whose sole purpose is for carrying out the transmission of a communication over a network, for example to identify the communication endpoints
- Example: load-balancing cookies that distribute network traffic across different backend servers, aka **session stickiness**
  - Here a load balancer **creates an affinity** between a client and a specific network server for the duration of a session using a cookie with a random and unique tracking id
  - Subsequently, for the duration of the session, the load balancer routes all of the requests of this client to a specific backend server using the tracking id

Session Stickiness

- Top image:
  - No load balancing at all
- Bottom image:
  - The LB generates and returns a tracking cookie back to a client when its session is initiated
  - This cookie is tagged to every subsequent client request and allows the LB to forward the request to always the same server (therefore the stickiness)



The *strictly necessary Exemption*

- Must be linked to a service delivered over the internet, i.e. a website or an app
- This service must have been explicitly requested by the user (i.e. typing in the URL) and the use of the cookie must be restricted to what is strictly necessary to provide that service
- Note that cookies related to advertising are not strictly necessary and must be consented to

Example for the *strictly necessary Exemption*

- A website uses session cookies to keep track of items a user places in an online shopping basket
  - Assuming this cookie will be deleted once the session is over
- Cookies that record a user's language or country preference

Data Processing

- Performing any operation on personal data, manually or by automate means, including:
  - Obtaining
  - Storing
  - Transmitting
  - Recording
  - Organising
  - Altering
  - Disclosing
  - Erasing

Entities in GDPR

- GDPR distinguishes between:
  - The Data Subject
  - The Data Protection Officer (DPO)
  - The Data Controller
  - The Data Processor

Mx5

NUI Galway
OÉ Gaillimh

The Data Subject

- This is the person to whom the data relates
  - GDPR only applies to living individuals
- However, any duty of confidence in place prior to the death extends beyond that point

The Data Protection Officer (DPO)

- The primary role of the DPO is to ensure that her organisation processes the personal data of its staff, customers, and other data subjects in compliance with the applicable data protection rules
- It is a mandatory role within three different scenarios:
  - When the processing is undertaken by a public authority or body
  - When an organisation’s main activities require the frequent and large-scale monitoring of individual people
  - Where large scale processing of special categories of data or data relating to criminal records forms the core activities
- The Data Protection Officer is required to be an expert within this field, along with the requirement for them to report to the highest management level.
  - With this being a challenging aspect of GDPR compliance for smaller organisations, there is the option to make an external appointment of a third-party

The Data Controller

- The Data Controller is the company or an individual who has overall control over the processing of personal data
- The Data Controller takes on the responsibility for GDPR compliance
  - A Data Controller needs to have had sufficient training and be able to competently ensure the security and protection of data held within the organisation

The Data Processor

- The Data Processor is the person who is responsible for the processing of personal information
- Generally, this role is undertaken under the instruction of the data controller
  - This might mean obtaining or recording the data, it’s adaption and use. It may also include the disclosure of the data or making it available for others
- Generally, the Data Processor is involved in the more technical elements of the operation, while the interpretation and main decision making is the role of the Data Controllers

Cloud Services and GDPR

- A Cloud Service Provider will be considered a **Data Processor** under GDPR if it provides data processing services (e.g. storage) on behalf of the Data Controller even without determining the purposes and means of processing
- A Cloud Service Provider that offers personal data processing services directly to Data Subjects will be **Data Controller**

Some Key Benefits for Data Subjects

- More information must be given to data subjects (e.g. how long data will be kept, right to lodge a complaint)
- Must explain and document legal basis for processing personal data
- Tightens the rules on how consent is obtained (must be distinguishable from other matters and in clear plain language)
- Must be as easy to withdraw consent as it is to give it
- Mandatory notification of security breaches without undue delay
  - To data protection commissioner within 72 hours

Personal Data Security Breaches

- Disclosure of confidential data to unauthorised individuals
- Loss or theft of data or equipment on which data is stored
- Hacking, viruses or other security attacks on IT equipment/ systems / networks
- Inappropriate access controls allowing unauthorised use of information
- Emails containing personal data sent in error to wrong recipient
- Applies to paper and electronic records

Some Key Benefits for Data Subjects

- Right of Access (copy to be provided within one month)
- Right to erasure (i.e. right to be forgotten)
- Right to restriction of processing
- Right to object to processing
- Right not to be subject to a decision based solely on automated processing

GDPR Overview

- The GDPR sets out several key principles:
  1. Lawfulness
  2. Fairness and transparency
  3. Purpose limitation
  4. Data minimisation
  5. Accuracy
  6. Storage limitation
  7. Integrity and confidentiality (security)
  8. Accountability

GDPR: Lawfulness

- You must **identify valid grounds** under the GDPR (known as a ‘lawful basis’) for collecting and using personal data
- Processing shall be lawful only if and to the extent that at least one of the following applies:
  - Consent
  - Necessary for the performance of a contract
  - Necessary for compliance with a legal obligation
  - Necessary to protect the vital interests of the data subject or another person
  - Necessary for the performance of a task carried out in the public interest
  - Necessary for the purpose of the legitimate interests

GDPR: Fairness and Transparency

- You must **use personal data in a way that is fair**; this means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned
- You must be **clear, open and honest with people** from the start about how you will use their personal data
- At the time personal data is being collected from data subjects, they must be informed via a "Data Protection Notice"

Data Protection Notice

- A data protection notice entails the following:
  - The identity and contact details of the data controller
  - The contact details of the data protection officer
  - The purpose of the processing and the legal basis for the processing
  - The recipients or categories of recipients of the data
  - Details of any transfers out of the EEA, safeguards in place and the means by which to obtain a copy of them
  - The data retention period used or criteria to determine same
  - The individual's rights (access, rectification and erasure, restriction, complaint)

GDPR: Purpose Limitation

- You must be **clear about what your purposes** for processing are from the start
- You need to **record your purposes** as part of your documentation obligations and specify them in your privacy information for individuals
- You **can only use the personal data for a new purpose** if either this is compatible with your original purpose, you get consent, or you have a clear basis in law

X

M

NUI Galway
OÉ Gaillimh

GDPR: Data Minimisation

- You must ensure the personal data you are processing is:
  - **adequate** – sufficient to properly fulfil your stated purpose
  - **relevant** – has a rational link to that purpose
  - **limited** to what is necessary – you do not hold more than you need for that purpose

GDPR: Accuracy

- You should take all reasonable steps to ensure the personal data you hold **is not incorrect or misleading** as to any matter of fact
- You may need to **keep the personal data updated**, although this will depend on what you are using it for
- If you **discover that personal data is incorrect or misleading**, you must take reasonable steps to correct or erase it as soon as possible
- You must **carefully consider any challenges to the accuracy** of personal data

(M)

NUI Galway
OÉ Gaillimh

GDPR: Storage Limitation

- You must not keep personal data **for longer than you need it**
- You need to think about – and be able to justify – **how long you keep personal data**; this will depend on your purposes for holding the data
- You need a policy **setting standard retention periods** wherever possible, to comply with documentation requirements
- You should also **periodically review the data you hold**, and erase or anonymise it when you no longer need it
- You must **carefully consider any challenges to your retention of data**; individuals have a right to erasure if you no longer need the data
- You can **keep personal data for longer if you are only** keeping it for public interest archiving, scientific or historical research, or statistical purposes

GDPR: Accountability and Governance

- Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that **you must be able to demonstrate your compliance**
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability

GDPR: Accountability and Governance

- Accountability requires controllers to maintain records of processing activities in order to demonstrate how they comply with the data protection principles, i.e.
  - Inventory of personal data
  - Providing assurance about compliance
  - Need to document
    - Why it is held
    - How it is collected
    - When it will be deleted
    - Who may gain access to it

GDPR: Integrity and Confidentiality

- A key principle of the GDPR is that you process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle’
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures
- Where appropriate, you should look to use measures such as **pseudonymisation and encryption**
- Your measures must ensure the ‘**confidentiality, integrity and availability**’ of your systems and services and the personal data you process within them
- The measures must also enable you to **restore access and availability** to personal data in a timely manner in the event of a physical or technical incident