

# CT437 COMPUTER SECURITY AND FORENSIC COMPUTING

THE CIA TRIAD  
REVISION: GDPR AND RAID

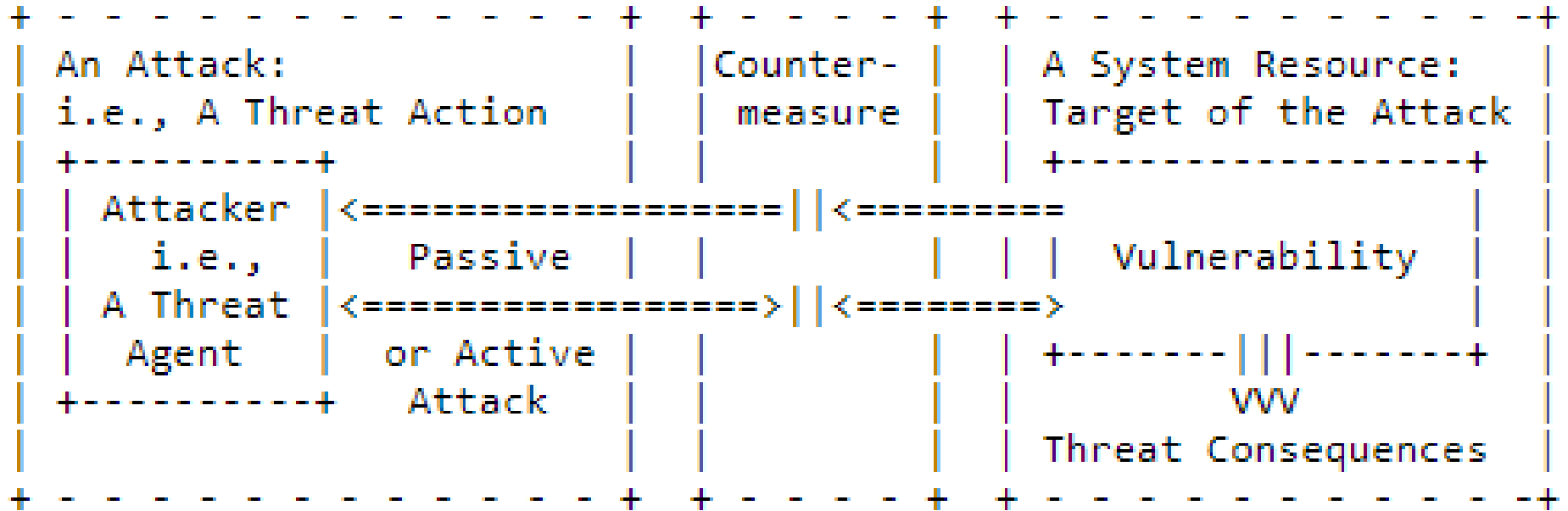
Dr. Michael Schukat



# Recap: RFC2828

2

- RFC2828, Internet Security Glossary
- <https://tools.ietf.org/html/rfc2828>



# Recap: Threat Consequences

3

- ❑ Threat consequences (as a result from a threat action) include
  - ❑ disclosure of information
  - ❑ Deception (i.e. pretending to be another entity)
  - ❑ disruption of services
  - ❑ usurpation, e.g. unauthorized control of some part of a system

- ❑ Cybercrime: it's all around us
  - Posing a major threat to personal and organizational data and even national security



Personal level

Your identity, data, and computing devices



Organizational level

Reputation, data and customers



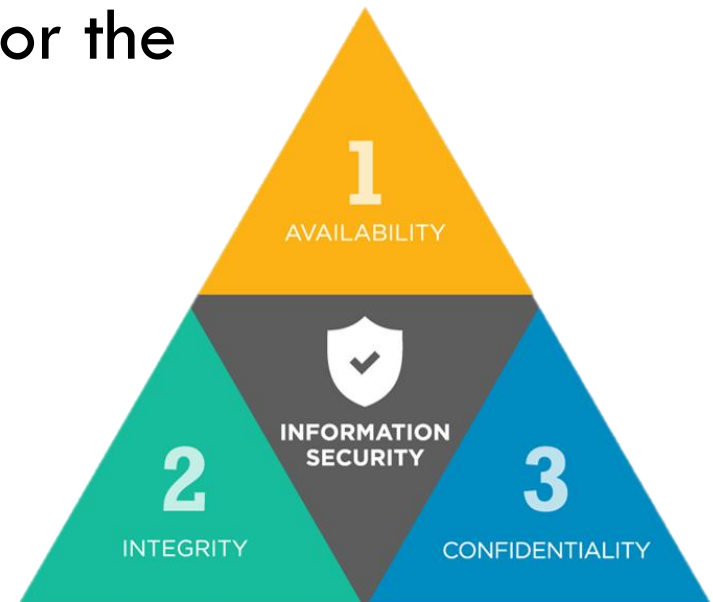
Government level

National security, economy and the safety of citizens

# The CIA Triad

4

- The three letters in "CIA triad" stand for
  - Confidentiality
  - Integrity, and
  - Availability
- It is a model that forms the basis for the development of security systems



# CIA Triad: Confidentiality

5

- ❑ *“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”*
- ❑ In layman's terms: Keeping things secret that are meant to be secret
- ❑ Protecting data at rest, in transit, and during processing / use



# Recall GDPR: 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"

# Recall GDPR: Sensitive Personal Data

- This includes
  - ▣ 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
  
- GDPR requires explicit consent to process special categories of personal data

# Compromising Confidentiality

8

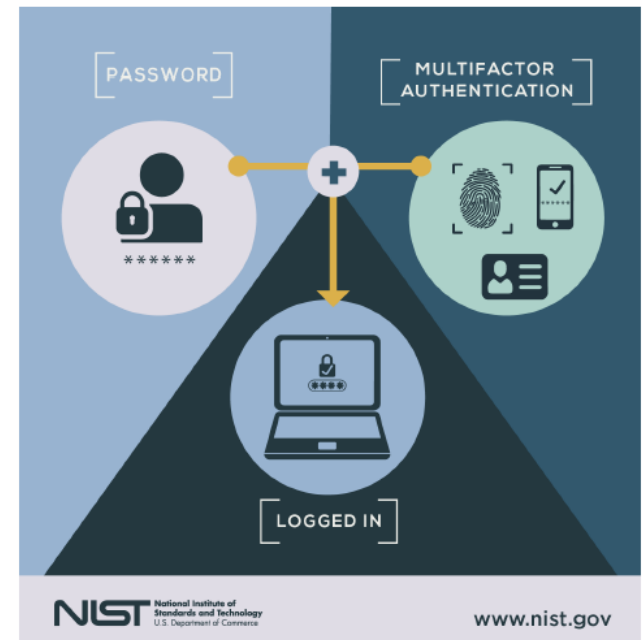
- Confidentiality can be compromised by various attacks, including:
  - ▣ Man-in-the-middle (MitM) attack
  - ▣ Escalation of privileges
  - ▣ Human error (weak password, sharing credentials etc.)
  - ▣ Insufficient security controls
  
- Can you identify situations where any of those attacks would apply?



# Technologies used to ensure Confidentiality

9

- These include:
  - ▣ Encryption (obviously)
  - ▣ Access Control (e.g. multi-factor authentication)
  - ▣ Secure network protocols
  
- Can you name a technology / protocol / algorithm that ensures confidentiality?



# CIA Triad: Integrity

10

- “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity”
  - ▣ Non-repudiation ensures that a party cannot deny having sent or received a message or transaction
  - ▣ Authenticity ensures that information and communication come from a trusted source; this includes protecting against impersonation, spoofing and other types of identity fraud
- In layman’s terms: keeping information accurate, complete, and protected from unauthorised modification
- Integrity makes sure that data is trustworthy and not tampered with
- Think of Revolut; can you provide an example for an attack on data integrity?

# Technologies to protect Integrity

11

- These include:
  - ▣ Network protocols that validate all data exchanged between end points
  - ▣ Digital signatures
  - ▣ Data hashes
  - ▣ Backup and data recovery strategies
  - ▣ Version control, to prevent the accidental change or deletion of information

# CIA Triad: Availability

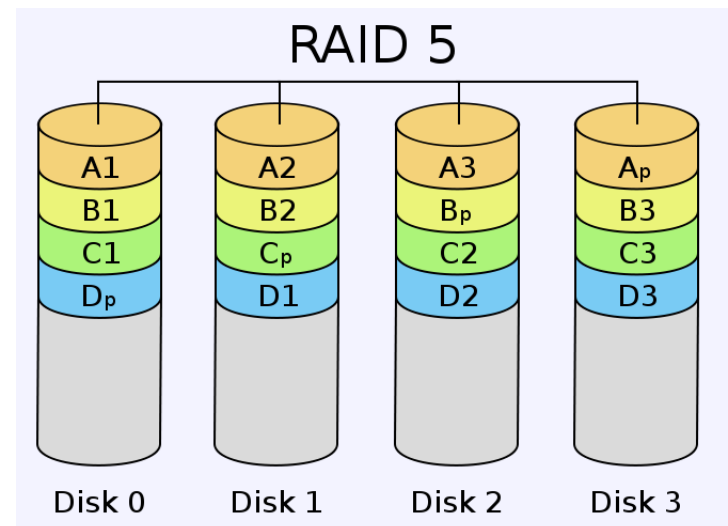
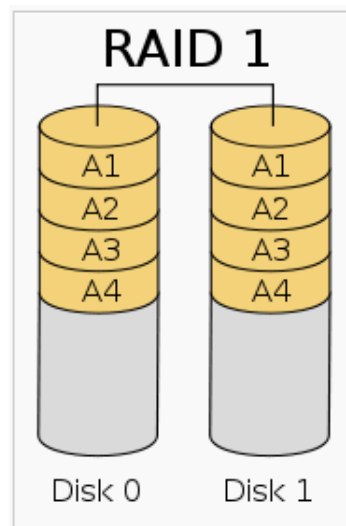
12

- “Ensuring timely and reliable access to and use of information”
- If data is kept confidential and its integrity maintained but it is not available to use, then it is often useless
- Availability can be compromised by various attacks, including:
  - ▣ (Distributed) Denial-of-service (DoS) attacks
  - ▣ Ransomware
  - ▣ Server overload
  - ▣ Physical incident such as a power outage or natural disaster

# Technologies to provide Availability

13

- These include:
  - ▣ RAID – Redundant Array of Independent Disks
  - ▣ Load balancers
  - ▣ Business continuity and disaster recovery plans, e.g., redundancy, failover, etc.

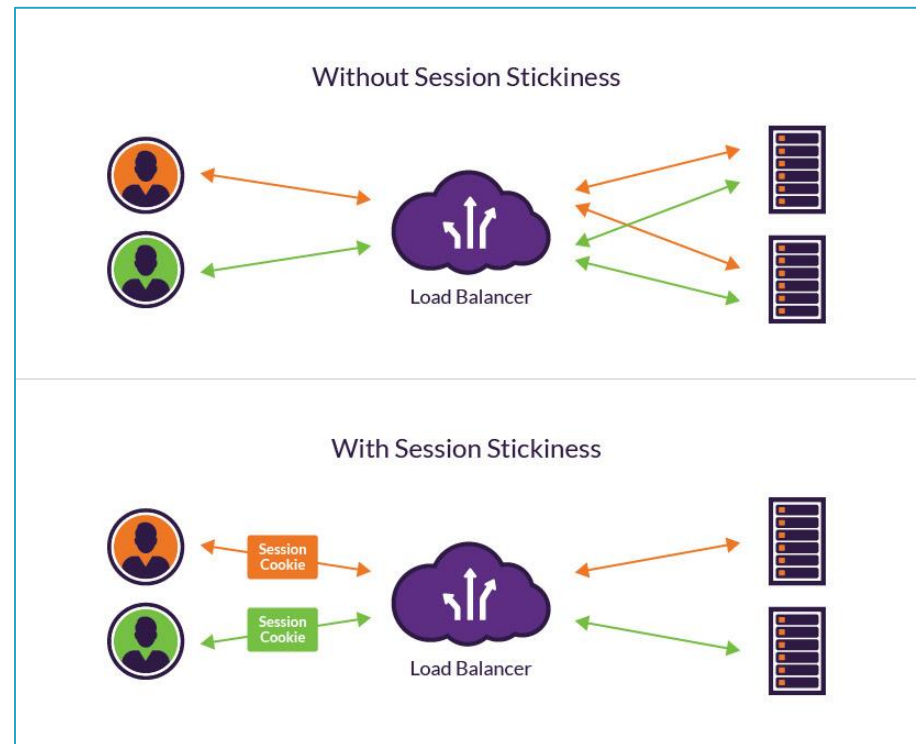


# Load Balancers

- Load balancers are server-side gateways that distribute client traffic between multiple backend (e.g., web-) servers
- They require load-balancing cookies on the client side that associate a client session with a particular server, aka **session stickiness**
- 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
- GDPR allows the unsolicited use of such cookies via the **communications exemption**

# Load Balancers

- ◆ Top image:
  - No load balancing at all
- ◆ Bottom image:
  - The LB generates and returns a tracking cookie back to a client when its first 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)



# Data Breaches

16

- ❑ Despite the best of intentions and all the safeguards one can put in place, protecting organisations from every possible cyber attack may not be feasible
- ❑ There is an on-going "arms-race" with cybercriminals constantly finding new ways to attack systems and, very often, they will succeed
- ❑ *"A data breach is defined as any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed"* (article 4.1 2 GDPR).



# CIA Triad Dependencies



17

- Each element connects with the others, and when you implement measures to ensure the protection of one, you must consider the ramifications it has elsewhere
- Example:
  - ▣ As a result of the recent cyberattack UoG implemented multi-factor authentication to access all services (email, student records, etc.)
  - ▣ Doing so protects the confidentiality of sensitive data, making it harder for unauthorised actors to compromise an employee's login credentials and view information using their account
  - ▣ However, without their mobile phone at hand, an employee can't complete the authentication process
  - ▣ This hampers therefore the availability of UoG services

# Risk Assessment

- ISO 27001 certification, GDPR compliance and other frameworks require the adoption of the CIA triad within an organisation
- All these standards mandate that organisations analyse their operations to measure the risks, threats and vulnerabilities in their systems that could compromise sensitive information
- This process is called **risk assessment**
- We may cover risk assessment at a later stage...

# Appendix / Revision

- RAID
- GDPR

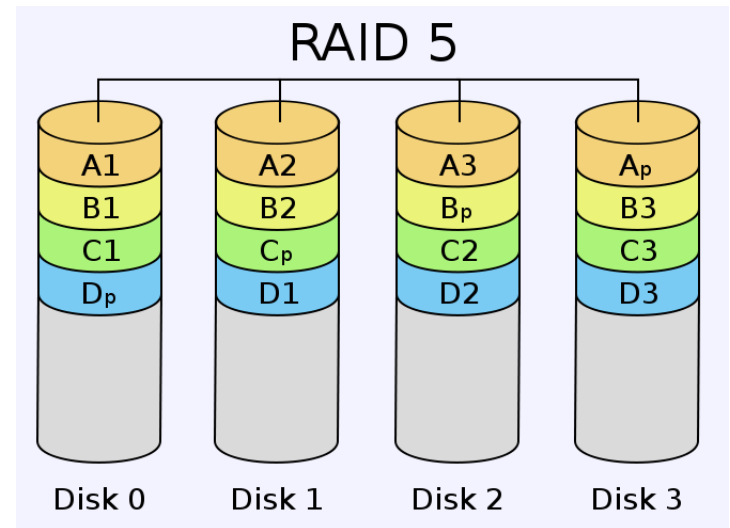
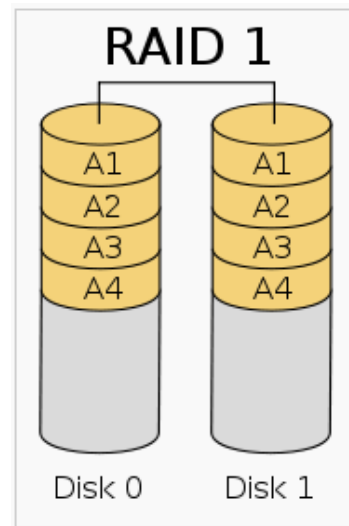
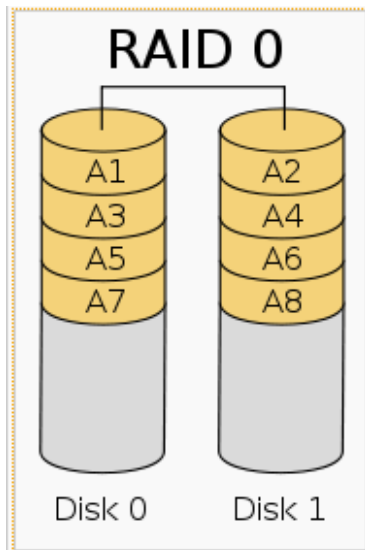
# Mass-Storage Redundancy via RAID

- ❑ Background: Hard disks are relatively slow (i.e. seek time + rotational latency) and as mechanical devices may fail
- ❑ Redundant Array of Independent Disks (RAID) is a data storage virtualisation technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy and / or performance improvement
- ❑ Data blocks are distributed across the drives in one of several ways, referred to as **RAID levels**, depending on the required level of redundancy and performance
- ❑ Many RAID levels use a parity-based error protection scheme (see RAID-4), example (with 12 bit / block):
  - ❑ Block 1:           010001101001
  - ❑ Block 2:           110011011010
  - ❑ Block 3:           000100100101
  - ❑ P Block:           100111010110 (bitwise EXOR, equivalent to even parity)



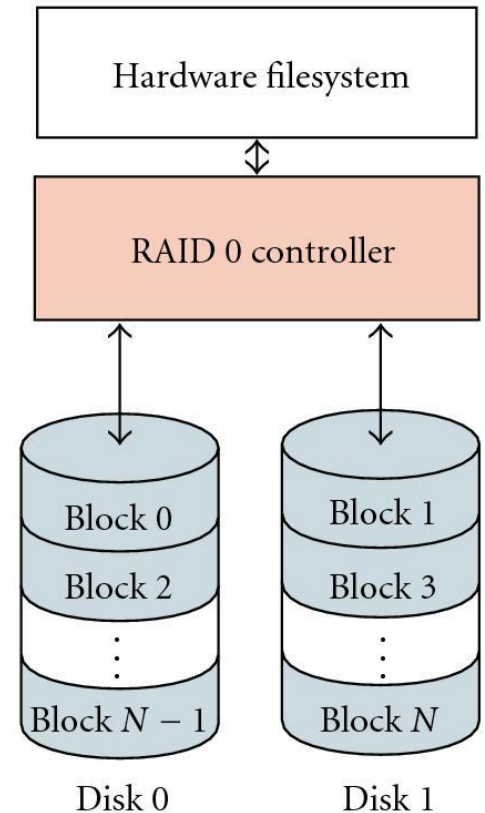
# Mass-Storage Redundancy via RAID

- ❑ RAID storage systems require a dedicated RAID controller, that supports the required RAID level
  - ▣ See also the diagram on the next slide
  - ▣ Normally such controllers are not shown in RAID diagrams



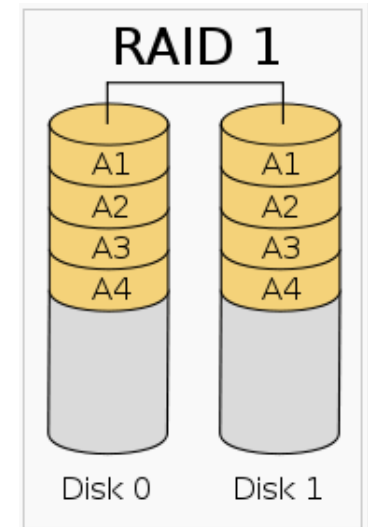
# RAID 0

- **Block-level striping without parity or mirroring**
  - ▣ **data striping** is the technique of segmenting logically sequential data, such as a file, so that consecutive segments are stored on different physical storage devices
- 2 or more drives (n) required
- **No redundancy**, but up to n-times R/W performance increase



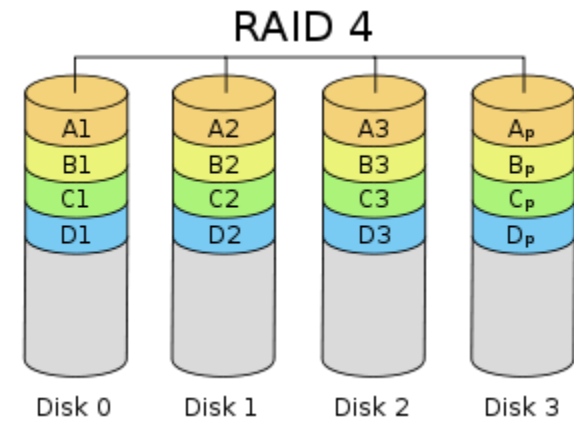
# RAID 1

- Block-level mirroring without parity or striping
- 2 or more drives (n) required
- (n - 1) drive failures can be compensated; here each disk can
  - ▣ diagnose catastrophic failures (e.g. head crash)
  - ▣ detect (but **not** correct) sector-wise bit errors on platters
- No increase in R/W performance



# RAID 4

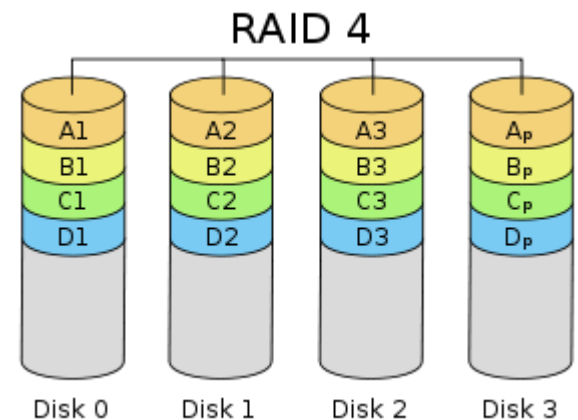
- ❑ Block-level striping with single parity disk
- ❑ Single catastrophic drive failure can be compensated (any drive can fail)
- ❑ RAID 4 provides good performance of random reads, while the performance of random writes is low due to the need to write all parity data to a single disk (Disk 3 in the diagram above)
- ❑ Minimum of 3 drives required





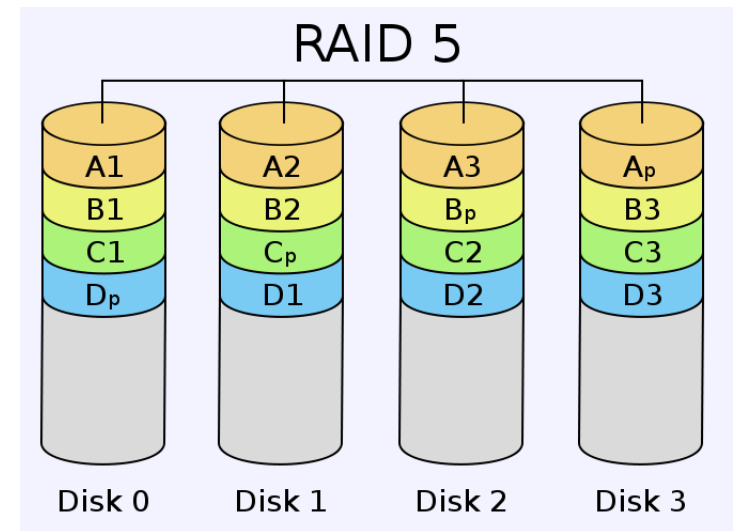
# Drive Hot-Swapping in RAID

- ❑ In RAID a defect drive will be (ASAP)
  - ❑ manually swapped for a new drive (hot-swap), or
  - ❑ replaced by an idle drive (hot-spare) already in the system
- ❑ The new drive's content is rebuild by the RAID controller while the disk set is still operational
- ❑ Example RAID 4 with Disk 0 swapped:
  - ❑  $A_1 = A_2 \text{ EXOR } A_3 \text{ EXOR } A_p$
  - ❑  $B_1 = B_2 \text{ EXOR } B_3 \text{ EXOR } B_p$
  - ❑  $C_1 = C_2 \text{ EXOR } C_3 \text{ EXOR } C_p$
  - ❑  $D_1 = D_2 \text{ EXOR } D_3 \text{ EXOR } D_p$



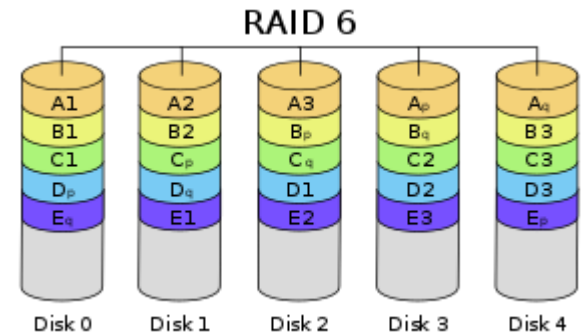
# RAID 5

- Similar to RAID 4, but:
  - ▣ Block-level striping with distributed parity
  - ▣ Distributed parity evens out the stress of a dedicated parity disk among all RAID members
  - ▣ Write performance is increased since all RAID members participate in the serving of write requests
- Minimum of 3 drives required



# RAID 6

- RAID 6 extends RAID 5 by adding another parity block
  - ▣ thus, it uses block-level striping with two parity blocks distributed across all member disks
- Double catastrophic drive failures can be compensated (any two drives can fail)
- Minimum of 4 disks required
- Second parity involves EXOR function (as seen before) and a bit shift function



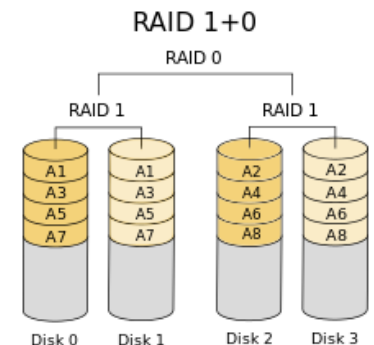
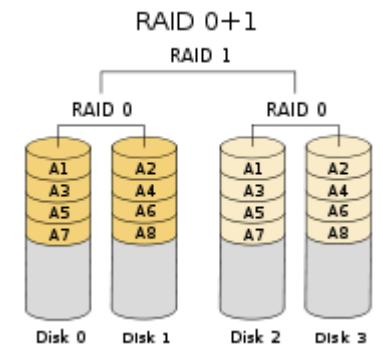
# Other RAID Levels

## □ RAID 0+1 (RAID 01)

- 4 drives minimum
- Some double catastrophic drive failures can be compensated

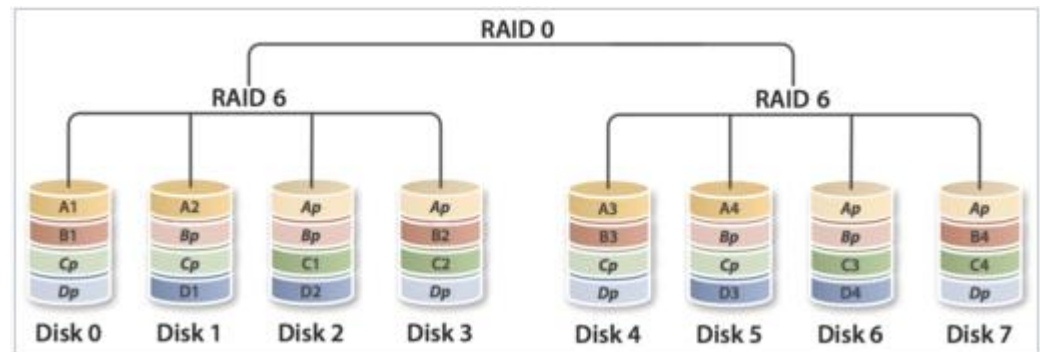
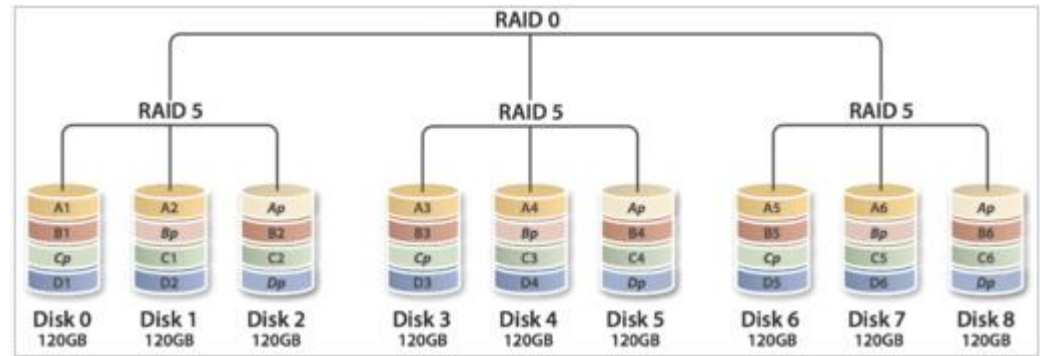
## □ RAID 1+0 (RAID 10)

- 4 drives minimum
- Some double catastrophic drive failures can be compensated
- Best throughput (apart from RAID 0), so preferable RAID level for I/O-intensive applications



# Other RAID Levels: RAID 5+0 (RAID 50) and RAID 6+0 (RAID 60)

- Some triple catastrophic drive failures can be compensated
- Rebuild-time after drive swap reduced because of controller hierarchy
  - ▣ Faster turnaround time to restore full I/O capacity
  - ▣ Shorter vulnerable period where a second drive failure would be catastrophic



# Summary RAID 0 – RAID 3

Level	Description	Minimum # of disks	Space Efficiency	Fault Tolerance	Read Benefit	Write Benefit	Image
RAID 0	Block-level striping without parity or mirroring.	2	1	0 (none)	nX	nX	<p>RAID 0</p> <p>Disk 0    Disk 1</p>
RAID 1	Mirroring without parity or striping.	2	1/n	n-1 disks	nX	1X	<p>RAID 1</p> <p>Disk 0    Disk 1</p>
RAID 2	Bit-level striping with dedicated Hamming-code parity.	3	$1 - 1/n \cdot \log_2(n-1)$	RAID 2 can recover from 1 disk failure or repair corrupt data or parity when a corrupted bit's corresponding data and parity are good.			<p>RAID 2</p> <p>Disk 0    Disk 1    Disk 2    Disk 3    Disk 4    Disk 5</p>
RAID 3	Byte-level striping with dedicated parity.	3	$1 - 1/n$	1 disk			<p>RAID 3</p> <p>Disk 0    Disk 1    Disk 2    Disk 3</p>

○

○

# Summary RAID 4 – RAID 6

Level	Description	Minimum # of disks	Space Efficiency	Fault Tolerance	Read Benefit	Write Benefit	Image
RAID 4	Block-level striping with dedicated parity.	3	$1 - 1/n$	1 disk			<p>RAID 4 diagram showing four disks (Disk 0 to Disk 3). Data blocks A1, B1, C1, D1 are striped across Disk 0, 1, 2, 3. Parity blocks A2, B2, C2, D2 are stored on Disk 3. Data blocks A3, B3, C3, D3 are striped across Disk 0, 1, 2, 3. Parity blocks A4, B4, C4, D4 are stored on Disk 3.</p>
RAID 5	Block-level striping with distributed parity.	3	$1 - 1/n$	1 disk	$(n-1)X$	variable	<p>RAID 5 diagram showing four disks (Disk 0 to Disk 3). Data blocks A1, B1, C1, D1 are striped across Disk 0, 1, 2, 3. Parity block A2 is on Disk 0, B2 on Disk 1, C2 on Disk 2, D2 on Disk 3. Data blocks A3, B3, C3, D3 are striped across Disk 0, 1, 2, 3. Parity block A4 is on Disk 0, B4 on Disk 1, C4 on Disk 2, D4 on Disk 3.</p>
RAID 6	Block-level striping with double distributed parity.	4	$1 - 2/n$	2 disks			<p>RAID 6 diagram showing five disks (Disk 0 to Disk 4). Data blocks A1, B1, C1, D1, E1 are striped across Disk 0, 1, 2, 3, 4. Parity blocks A2, B2, C2, D2, E2 are stored on Disk 1, 2, 3, 4, 0. Data blocks A3, B3, C3, D3, E3 are striped across Disk 0, 1, 2, 3, 4. Parity blocks A4, B4, C4, D4, E4 are stored on Disk 1, 2, 3, 4, 0.</p>





# 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

# GDPR in Ireland

- GDPR applies to the majority of personal data processing tasks, but further rules on certain issues (for example the reasons for, and extent to which, data subject rights may be restricted) are set out in the **Data Protection Act 2018**
- Further on, the **Law Enforcement Directive** concerns the processing of personal data by law enforcement, i.e., the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

# 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

# Recall GDPR: 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"

# Recall GDPR: Sensitive Personal Data

- This includes
  - ▣ 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
  
- GDPR requires explicit consent to process special categories of personal data

# Recap 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](http://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

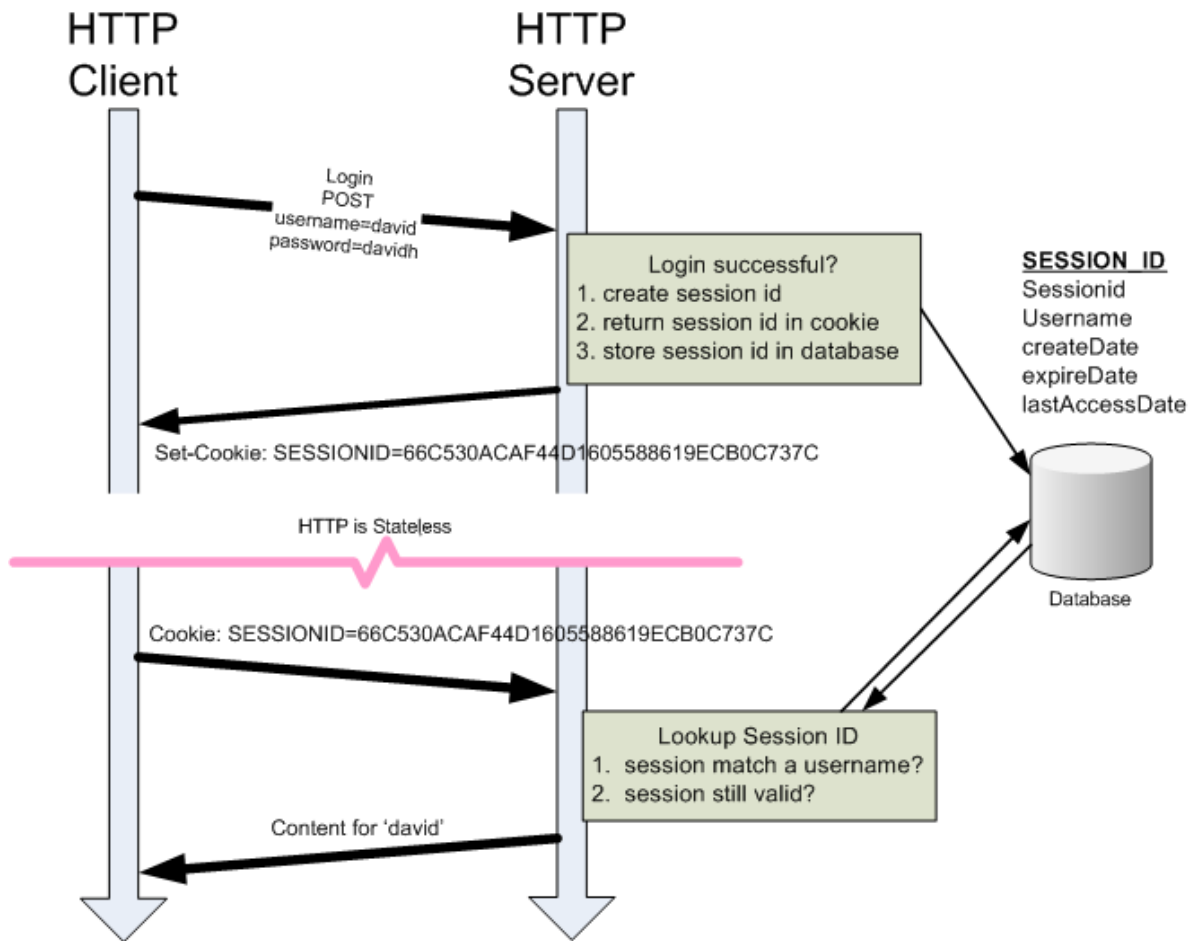
- A session cookie (aka in-memory cookie, transient cookie or non-persistent cookie) exists only in temporary memory while the user navigates its website
- Web browsers normally delete session cookies when the user closes the browser
- Session cookies do not have an expiration date assigned to them, 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

44



# Cookie Attributes

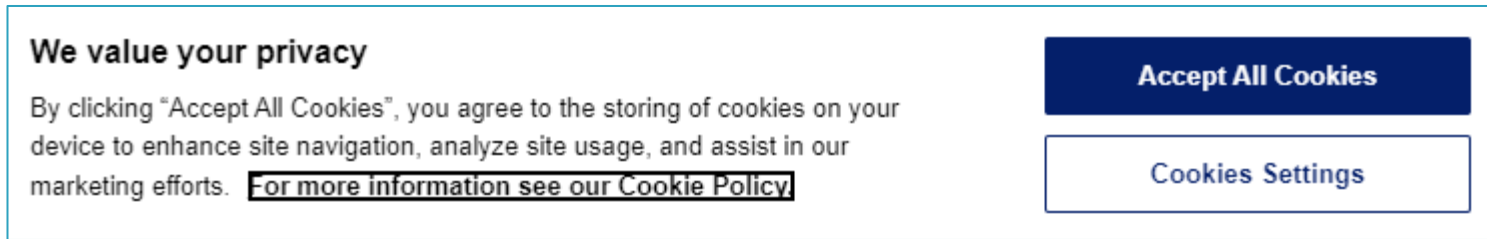
- Consider the following response header sent by a webserver that contains 3 persistent cookies:

```
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

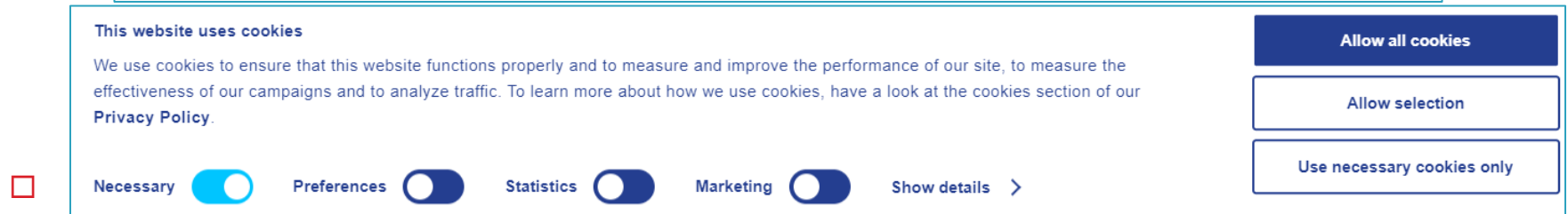


**We value your privacy**

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](#)

**Accept All Cookies**

Cookies Settings



- **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  Show details >

**Allow all cookies**

Allow selection

Use necessary cookies only

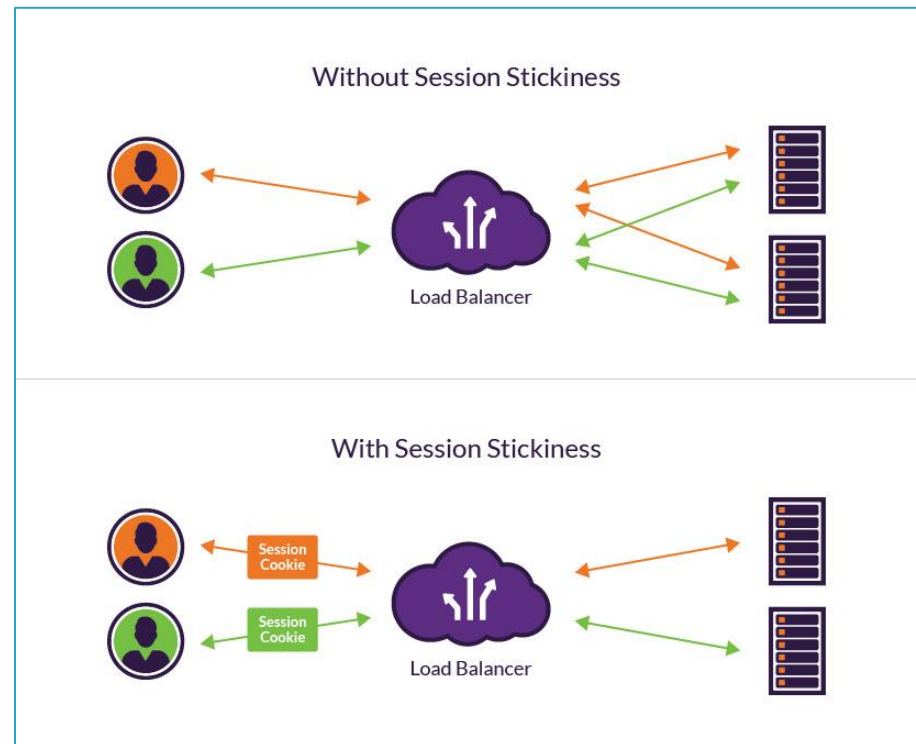
- The communications exemption
- The strictly necessary exemption

# 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

# The Data Subject

- This is the (living!) person to whom the data relates
- Under GDPR, businesses have a legal obligation to keep their data up-to-date, which means that, theoretically, data of deceased should be removed
- Deceased persons, who predate the introduction of GDPR, may be covered by national legislation active at the time of death (e.g. the Data Protection Acts 1988 and 2003 in Ireland)
- Access by a next-of-kin to the personal data (e.g. emails) of a deceased person may be possible under Irish **Freedom of Information laws**

# 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, its 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 Key Principles

- 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 Principle: 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 Principle: 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 Principle: 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

# GDPR Principle: 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 Principle: 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

# GDPR Principle: 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 Principle: 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 Principle: 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 Principle: 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