# Introduction to: Data Protection Act & GDPR

Used as a guide for
Junior Developer Group

# Why should you care about data?

# What is...Data Protection Act?

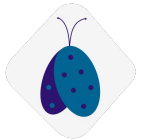
# The Data Protection Act 2018

The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK.

**The Data Protection Act 2018 aims to:**

Prevent people or organisations from holding and using inaccurate information on individuals.

This applies to information regarding both, private lives or business.



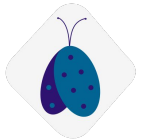
# What does GDPR mean?

# The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a legal framework which sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU) and EEA areas .

It establishes obligations for businesses and provides rights for citizens and also addresses the transfer of personal data outside the EU and EEA areas

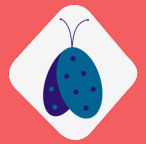
It enforces ‘Opt-In’ rather than ‘Opt-Out’ behaviour when collecting data.




What would be a way of companies show their data protection laws compatibility to users/customers?

🤔🤔🤔

# The Eight Principles of: Data Protection



# 1. Fair and lawful

Organisations must have legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn't expect

## Organisations are required to:

- Provide full transparency about how they wish to use the data.
- Ensure their data is only used in ways customers would expect.
- Specify in which way information is being used.
- Allow users to make an informed decision as to whether to share certain pieces of personal information.

# 2. Specific of its purpose

Organisations must be open about their reasons for obtaining personal data and what they plan to use it for.

## Organisations are required to:

- only use the personal data for the purpose they originally said it would be used for.
- should not use the data to market other companies to their customers unless the individual has agreed to it.
- unless they have agreed, an organisation cannot use their customers' details to promote other companies, including internal/umbrella companies.
- shouldn't pass customers' details onto third parties unless the customers have already consented to it.

# 3. Use information only for what is needed

The data organisations hold on their customers should be adequate for the purpose they are holding the information for

## Organisations are required to:

- avoid holding more information than necessary for their customers
- have privacy notices or “how we use your information” guides written clearer than before.
- inform customers of exactly what their data is being used for
- must inform the customer of their right to withdraw consent at any time.

# 4. Information kept accurate and up to date

Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate

## Organisations are required to:

- stop contacting the individual using the previously provided details when a customer updates the information a company holds on them

- should not simply wait for individuals to contact them to update their information, they should be active in ensuring they have the correct information on an individual.

# 5. Not kept longer than needed

Organisations must regularly review the length of time they retain data on individuals, keeping  data for the amount of time required will make it easier to return personal information to customers that request it.

## Organisations are required to:

- properly destroy or delete data that is out of date or no longer necessary or required to be removed by the customer

- retain enough information on the individual to ensure they can remove customers from their marketing lists when requested.

# 6. Take into account people's rights

People have the right to access their personal data, stop it from being used if it is causing distress, prevent it from being used for direct marketing, have inaccurate data changed, and claim compensation for damaging data breaches.

- Customers have the right to request that specific data be deleted or destroyed properly destroy or delete data that is out of date or no longer necessary or required
- Customers should only request information relevant to themselves
- Customers can request to see the information held on them by submitting a subject access request. This is a request typically sent by email, online forms or post.

# 7. Kept safe and secure

A proper physical and technical security system must be used to keep personal information safe and secure, and not be exposed to security risks.

- It is advisable to provide training for staff in the organisation on data protection and cyber security
- Each organisation should evaluate potential repercussions of a data breach

# 8. Not be transferred

Data should not be transferred to other systems, even countries, that do not have the same level of data protection.

- Data protection officers, risk managers and those involved in processing and distributing data should become familiar with these principles in order to ensure their organisation is compliant

**Example**:
the EU has a ‘Privacy Shield’ that American companies can sign up for to enable data to be legally sent across the Atlantic.

Data sent within the EEA and a few other specified countries is allowed.

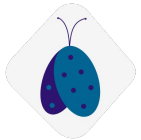

Can you think of any data violation examples, both in tech and non-tech organisations? 🤔

# What are we responsible for?

As people interested in, or working in tech,
we'll often be a part of Data Collection
and Data Management tasks.

While as individuals we will (now) be more
aware of the ways our data is being used and
careful of which information we share with others.

Considering the above, our responsibility is being aware
of the current rules and regulations, enforcement of them
and reporting of potential violations.



# What advice could you give to others?

- You could advise to find more information on any Electronic Communications Regulations laws for their location
- You could advise to send a request to view all collected data to the organisation in question
- You could advise sending a complaint with a national Data Protection Authority (DPA)
- You could advise sending a report of a data breach to ICO

# Well Done!

You've now learned a bit more about Data Protection, why should we care about it what we can do to report violations to proper authorities who are able to help us deal with situations we might find ourselves in.


**Likii,**
**Junior Developer Group**