

# Keeping organisational data secure



Worksheet section	Contents
1	Data breaches
2	GDPR
3	Technology to protect data

Version: 1.0

This lesson has been created by effini in partnership with Data Education in Schools and Skills Development Scotland.

© 2022. This work is licensed under a [CC BY-NC-SA 4.0 license](#).



You are free to:

**Share** – copy and redistribute the material in any medium or format

**Adapt** – remix, transform and build upon the material

Under the following terms:

**Attribution** — You must give [appropriate credit](#), provide a link to the license, and [indicate if changes were made](#). You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

**NonCommercial** — You may not use the material for [commercial purposes](#).

**ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the [same license](#) as the original.

**If you require this document in an alternative format, such as large print or a coloured background, please contact**

**hello@effini.com**

**or**

**4th Floor, The Bayes Centre  
47 Potterrow  
Edinburgh  
EH8 9BT**

# 1. Data breaches

## Section 1.1 (recall)

- 1) Fill in the missing words for this definition of a data breach.

An incident that has affected the  of personal data.

- 2) It is important to organisations to keep data secure. State 2 consequences to an organisation if they don't keep personal data secure

## Section 1.2 (apply)

An employee has accidentally sent an email containing un-encrypted names and email addresses of their customers who have bought one of their products to a competitor.



The scenario above is an example of data breach.  
Thinking about this scenario, answer these questions.

- 3) What personal data was shared?

- 4) Who might benefit from this data breach?

- 5) What could be the impact on the company of this data breach?

- 6) What do you think could happen to the employee who send the email?

## 2. GDPR

### Section 2.1 (recall)

1) Match these definitions against the words below.

Regulation that governs the **way that organisations can use**, process and store

**Determines why and how personal data** is processed in an organisation

The identified or identifiable living individual **to whom the personal data relates**.

**Information that tells individuals** how an organisation will use, store or share their personal data

	Definition
GDPR	
Privacy notice	
Data subject	
Data controller	

### Section 2.2 (rephrase)

2) As a data subject you have rights under GDPR. Can you fill in the gaps for the benefits you have from these rights?

GDPR right	Benefit as a data subject
Right to be informed	You can find out what personal data a company has and how they are using it
Right of access	
Right to rectification	The data has to be accurate, if its not you can ask for it to be fixed.
Right to erasure	
Right to restrict processing	You can ask for a limited use of your data
Right to data portability	
Right to object	
Rights in relation to automated decision making and profiling	You can have decisions made by a real person rather than an automated system.

## 2. GDPR

- 3) Imagine you are working for a company that has the email addresses for people who wish to receive updates about a festival that is happening in their town. When sharing their email addresses, the people were told their details would only be used to receive information about the festival.



Your company is also promoting a new coffee shop and wants to tell people about it.

Imagine you are working as a data controller in the company, which of these do you think you should allow?

	Yes/No	Why?
Share the email addresses with the coffee shop owners as they will be useful to them.		
Look at the age/gender/address of the people signed up and only email people you think might like to hear about the coffee shop.		
Only send emails to these people about the festival not the coffee shop.		

- 4) Under GDPR you have the right to be forgotten. Can you think of some reasons why you might want a company to delete data they hold about you?

### Section 1.2 (active)

- 5) As a data subject you have the right to be informed about the data an organisation holds about you. Many organisations allow you to download the information they hold.

Think about an organisation that holds data about you, then search online to fill in a subject access request to see the information they hold about you.

Here are some websites you could use,

Facebook <https://www.facebook.com/help/contact/>

Twitter <https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data>

Snapchat <https://support.snapchat.com/en-US/a/download-my-data>

WhatsApp <https://faq.whatsapp.com/general/account-and-profile/how-to-request-your-account-information>

## 2. GDPR

---

Apple <https://support.apple.com/>  
Microsoft <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-manage-gdpr-data-subject-requests-with-the-dsr-case-tool>  
Instagram <https://help.instagram.com/contact/>

Which organisation have you contacted with a subject access request?

What did you have to do? e.g. did you have to prove your identity? Did you have to fill in a form?

You might have to wait to receive your data. How long did it take for you to get it?

Have you received your data? If you have, did it look correct?

### 3. Technology to protect data

#### Section 3.1 (recall)

- 1) Which of these statements about encryption are true?

Statement	True/False
Encryption is encoded using a key.	
If I encrypt my data I will never be able to read it again.	
Encryption is only for data that is in transit.	
The main way to keep data safe is to encrypt it.	

#### Section 3.2 (rephase)

- 2) Thinking about ways to keep organisational data secure. Why should an organisation use these methods to protect personal data?

Method	Why?
Backing up data and code	
Limiting access	
Testing and monitoring	

#### Section 3.3 (active)

- 3) End to end encryption is where the only the sender and receiver can view the message - not even the organisation you are using to send the message can't read it. Think about the services you use to transmit your personal data, (e.g. messages, photos), then research online to find out if they use end-to-end encryption.

Here are some websites that might help you,  
WhatsApp <https://www.whatsapp.com/security>  
Facebook <https://www.facebook.com/help>

Other message sharing organisations you could research are: Twitter, Snapchat, Steam, Zoom.

### 3. Technology to protect data

---

Which organisation have you researched?

Do they use end to end encryption to transmit your data?

What does this mean for any messages/photos you might send through this organisation?