



GDPR STAFF AWARENESS TRAINING

An Acumenology Business Guide
Acumenology.co.uk | All rights reserved

Published 2020

Welcome to your training on the General Data Protection Regulation or GDPR

This course provides information on the new GDPR regulation which came into force on the 25th May 2018.

The purpose of the course is to provide employees of an organisation an understanding of the regulations and how it affects the business.

Training is also an essential element of compliance to ensure employees have adequate knowledge of the GDPR.

[BACK](#)

DISCLAIMER The information contained herein was prepared by Raj Tandon and the information presented was correct at the time of publication in 2018. You should not rely on the information presented as a basis for making any business, legal or other decisions.

[NEXT](#)

The Course covers



Module 1
Introduction to
the GDPR



Module 2
The GDPR
Principles



Module 3
Rights of
Individuals



Module 4
Why Compliance
Matters

By the end of the course participants will be able to:

- ⚡ Understand the purpose of the GDPR
- ⚡ Explain what information falls under the GDPR
- ⚡ Have the knowledge to manage and implement the GDPR
- ⚡ Know the rights data subjects have under the GDPR
- ⚡ Be aware of consequences of failure to comply

BACK

NEXT

Module 1

Introduction to the GDPR

[BACK](#)

[NEXT](#)

Module 1 Covers



What is the GDPR?



Why is it important?



Who does it affect?



What is personal data?



What is processing?



Who does GDPR apply to?



The supervisory authority



Summary

BACK

NEXT

The GDPR (General Data Protection Regulation) is new EU legislation that came into force on the 25th May 2018

What does it do?

Protects the rights of EU subjects and gives them more control over how their personal information is collected and processed.

Simplifies and unifies regulations across the EU.

Requires organisations to demonstrate compliance with the GDPR principles by adopting appropriate policies, procedures and processes to protect the personal data they hold.

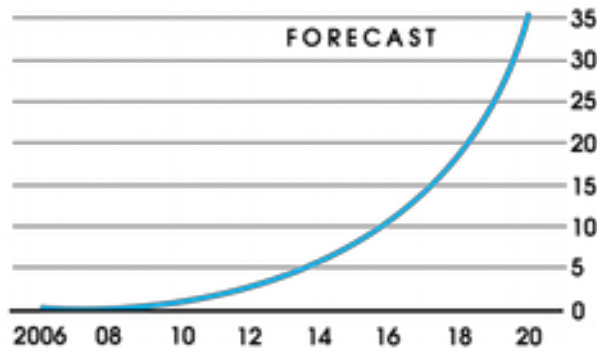
[BACK](#)[NEXT](#)

Technology has evolved and now plays an integral part in our lives



Too much Information

Worldwide digital data created and replicated Zettabytes*



[BACK](#)

World's Largest Companies by Market Cap

Accurate as of July 29, 2016 (10:50am ET)

Apple	\$567.75 billion
Alphabet	\$546.49 billion
Microsoft	\$445.14 billion
Amazon	\$366.95 billion
Facebook	\$364.26 billion

[NEXT](#)

The GDPR applies to any organisation that processes any personal data of anyone who resides in the EU

The GDPR applies to any organisations that collect and process any personal data of EU citizens irrespective of their location and, regardless of where that organisation is, or where the processing takes place.

Thus, a company outside the EU targeting consumers within the EU will be subject to the GDPR.

[BACK](#)[NEXT](#)

Under the GDPR personal data is any information about an identifiable, living person

An identifiable individual is one who can be identified by anything such as:



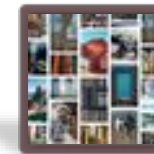
Name



Email address



Posts on
social media



Photographs



Photo



Bank details



Medical
information



CCTV

It's also applies to data that could be combined with other information to find something out about a person and is thus classified as personal information.

[BACK](#)[NEXT](#)

Some personal data is considered more sensitive than others

The special categories of data include data which reveals:



Racial or ethnic origin



Political opinions



Religious or philosophical beliefs



Trade-union membership



Genetic data



Biometrics



Data concerning health, sex life,
including sexual Orientation



Data about children under the age of 16
requires special protection, as they are
particularly vulnerable

BACK

NEXT

Processing is anything you do with personal data

Processing includes any of the following activities:



Collecting and recording data



Using data



Disclosing data



Holding data even if it involves doing nothing with it



Retrieving data



Erasing data

The GDPR protects all personal data from anything you're likely to do with it, making sure it's only used in the way the person whose data it is has agreed to.

[BACK](#)[NEXT](#)

Any organisation that processes the personal data of anyone who resides in the EU, even if the processing takes place elsewhere

The GDPR applies to ALL organisations processing the personal data of anyone who lives in the EU, regardless of where that organisation is, or where the processing takes place.

Thus, a company outside the EU but which does business in the EU is subject to the GDPR.

[BACK](#)[NEXT](#)

The Information Commissioner's Office (ICO) is the Supervisory Authority for the UK

Every country in the EU has its own supervisory authority and the ICO is the UK's.

It is an independent regulatory authority whose mission is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals".

[BACK](#)[NEXT](#)

Learnings in this module:



Understanding the GDPR

The GDPR is new EU legislation that protects the rights of EU subjects and gives them more control over how their personal information is processed. It applies to any organisation that processes the personal data of anyone who resides in the EU, even if the processing takes place elsewhere.



Personal Data

Personal Identifiable Information is any information about an identifiable living person.



Supervisory Authority

The Information Commissioner's Office or ICO is the Supervisory Authority for the UK.

[BACK](#)[NEXT](#)

Module 2

The GDPR Principles

[BACK](#)

[NEXT](#)

Module 2 Covers



Data protection terminology



The GDPR principles



Summary

BACK

NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



Data Protection
Officer



BACK

NOTE:

Click on the box to show
meaning of the word



Erasure



Personal Data



Processor



Processing



SAR (Subject
Access Request)



NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



BACK

A freely given specific, informed, and explicit agreement by the data subject to allow an organisation to process their personal data. Consent is the foundation of the GDPR.



Erasure



Personal Data



Processor



Processing



**SAR (Subject
Access Request)**



NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



It may be organisations or individuals who collect and process the personal data for legitimate purposes. Since a company is a separate legal entity, it is normally the data controller rather than an individual who is a part of the company.



Erasure



Personal Data



Processor



Processing



**SAR (Subject
Access Request)**



BACK

NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



Erasure



Personal Data



Processor



Processing



**SAR (Subject
Access Request)**



A breach of security
leading to the accidental or unlawful
access to, destruction, misuse etc.
of personal data.

BACK

NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



A person whose personal data is collected and processed by an organisation. It can include individual customers, employees and third-party suppliers.



Erasure



Personal Data



Processor



Processing



**SAR (Subject
Access Request)**



BACK

NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



A data security
and protection expert whose job is to
ensure an organization sustains
GDPR compliance.



Erasure



Personal Data



Processor



Processing





**SAR (Subject
Access Request)**







BACK



NEXT



The following terminology is essential for your understanding of GDPR

 **Consent** 



 **Controller** 



 **Data Breach** 



 **Data Subject** 



 **Data Protection Officer** 



Also known as the
'Right to be Forgotten', it entitles
the data subject to have the
controller erase
GDPR compliance.
personal data.

 **Erasure** 

 **Personal Data** 

 **Processor** 

 **Processing** 

 **SAR (Subject Access Request)** 

[BACK](#)

[NEXT](#)



The following terminology is essential for your understanding of GDPR







[BACK](#)



[NEXT](#)



The following terminology is essential for your understanding of GDPR

 **Consent** 

 **Controller** 



 **Data Breach** 



 **Data Subject** 



 **Data Protection Officer** 



Organisations or individuals who process data on behalf of the controllers. For example, an outsourced service provider such as payroll, HR. Employees of the controller are not considered as processors



GDPR compliance

 **Erasure** 

 **Personal Data** 

 **Processor** 

 **Processing** 

 **SAR (Subject Access Request)** 

BACK

NEXT

The following terminology is essential for your understanding of GDPR



Consent



Controller



Data Breach



Data Subject



**Data Protection
Officer**



Erasure



Personal Data



Processor



Processing



**SAR (Subject
Access Request)**





Any operation
that is done to, or with, personal
data, including collecting, using,
storing or deleting.



GDPR compliance



BACK



NEXT



The following terminology is essential for your understanding of GDPR

 **Consent** 



 **Controller** 



 **Data Breach** 



 **Data Subject** 



 **Data Protection Officer** 



A request
by the data subject for access to
the personal data held by the
Data Controller.

 **Erasure** 

 **Personal Data** 

 **Processor** 

 **Processing** 

 **SAR (Subject Access Request)** 

BACK

NEXT

The seven principles set out the main responsibilities for organisations



Fair, Lawful and
Transparent Processing



Purpose Limitation



Data Minimisation



NOTE:

Click on the box to
show meaning



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Fair: Processed as it has been described.
Lawful: Processed lawfully as described in the GDPR.
Transparent: Tell the subject what data processing will be carried out.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Data can only be used for the specific purpose the data subject has been made aware of. It cannot be used for another purpose without further consent.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Personal data collected shall be adequate, relevant and limited to what is necessary for the purpose for which it is processed.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Data must be “accurate
and where necessary kept up
to date”.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Data should not be kept for longer than is necessary and should be removed if no longer required.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



Controllers are responsible for the security of the data they collect. This includes security of the data when it is being processed by a third party.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

The seven principles set out the main responsibilities for organisations



**Fair, Lawful and
Transparent Processing**



Purpose Limitation



Data Minimisation



The controller is responsible for, and be able to, demonstrate compliance with the principles.



Accurate & Up to Date



Storage Limitation



Integrity & Confidentiality



Accountability



BACK

NEXT

Fair

We must be open and honest about who we are and how we will process someone's personal data. We must only handle it as they would reasonably expect and we mustn't have an unjustifiably negative effect on them.

Lawful

We must have a legal basis before we can process personal data. These include:

- Consent The individual has consented
- Contractual necessity It's necessary so an individual can enter into a contract or in relation to an existing contract.
- Legal compliance It's necessary for our compliance with legal obligations.
- Vital interests It's necessary to protect the vital interests of the data subject or another natural person e.g. in cases of life or death.
- Public interest It's necessary to deliver justice, or to exercise statutory, governmental, or other public functions.
- Legitimate interests It's in accordance with the data controller's legitimate interests, e.g. a finance company who use an agency to locate a client.

Transparent

A clear and complete privacy notice tells people exactly how we will use their data.

[BACK](#)[NEXT](#)

Data can only be used for the specific purpose the data subject has been made aware of

We must only collect personal data for the purpose it was collected for. We cannot collect it for one reason and then decide at a later stage to use it for another reason. If you decide to use it in a different way, you will need to obtain further consent.

Example

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

To comply, keep these in mind

- Be clear and transparent about why you are collecting the data.
- Don't use the data for anything else without first obtaining consent.

[BACK](#)[NEXT](#)

Personal data collected shall be adequate, relevant and limited to what is necessary for the purpose for which it is processed

You can only ask for information which is relevant to the reason you're collecting it. This means that you can't ask for information simply because it might be useful in the future.

Your organisation should have regular reviews, looking at the data they're asking for and checking it's still necessary to complete their intended purpose.

Example

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

[BACK](#)

To comply, keep these in mind

- Is this the minimum amount of data I need?
- Do I have enough information?
- Does it all apply directly?
- Is any of this information 'just in case' or 'might be useful'?

[NEXT](#)

Data must be “accurate and where necessary kept up to date”

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

Be careful when you take the details, make sure the correct information is collected. The GDPR gives people the right to request that their data is changed, completed, corrected or deleted. So, your organisation needs a clear procedure to do this.

Your organisation should also have a procedure in place to check that data is up-to-date.

Example

If an individual moves house from London to Manchester a record saying that they currently live in London will obviously be inaccurate. However a record saying that the individual once lived in London remains accurate, even though they no longer live there.

To comply, keep these in mind

- Whether the data is likely to change?
- How often it might and therefore how often you should check?
- How you can maintain accuracy efficiently and reliably?

[BACK](#)[NEXT](#)

Data should not be kept for longer than is necessary and should be removed if no longer required

You should only keep personal data for as long as it's needed and must be deleted when it is no longer needed for the purpose it was collected..

Your organisation should have procedures in place to check if you still need to keep the data and a procedure to securely delete information if not.

You can't keep hold of data on the off-chance that it may be useful in the future.

Example

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

To comply, keep these in mind

- When and how should personal data collected be destroyed?
- Should data be retained or disposed?

[BACK](#)[NEXT](#)

Controllers are responsible for the security of the data they collect. This includes security of the data when it is being processed by a third party

Personal data must be kept safe and secure and should be protected from accidental or deliberate loss, destruction, damage or unauthorised access.

An organisation needs to know how to keep data safe and have a robust IT security policy.

To comply with this principle:

- Develop a robust IT security policy
- Follow procedures such as setting safe passwords, encrypt laptops to prevent unauthorised access

[BACK](#)[NEXT](#)

Accountability is key principle and compliance with the GDPR must be demonstrated

The GDPR states that organisations must be able to demonstrate compliance with the Data Protection Principles.

Make sure you know what your organisations' policies and procedures contain and how they're used.

To comply you must:

- Follow your data protection and information security policies
- Maintain data protection documentation

Remember the ICO can audit and check an organisations compliance through this documentation.

[BACK](#)[NEXT](#)

Learnings in this module:



Terminology

Controller is the person or entity who determines the purpose and means of processing personal data. The company as a whole is normally the data controller.



GDPR Principles

There are seven principles that an organisation must adhere to:

1. Fair, lawful and transparent processing
2. Purpose limitation
3. Data minimisation
4. Accurate & up to date
5. Storage limitation
6. Integrity & confidentiality
7. Accountability which requires documented evidence of compliance with the principles

[BACK](#)[NEXT](#)

Module 3

Rights of Individuals

[BACK](#)

[NEXT](#)

Module 3 Covers



The rights of the individual
under GDPR



Summary

BACK

NEXT

The GDPR sets out the rights people have over their personal data

NOTE: Click on box for further details or
click next for more details



Right to be informed



Right of access



Right to rectification



Right to erasure



Right to restrict processing



Right to data portability



Right to object



Rights to Automated Decision -
Making and Profiling



BACK

NEXT

We must inform individuals how we use their data

We must inform data subjects about the collection and processing of their personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

This is done through a privacy notice, welcome letter or terms and conditions of engagement.

The information should include:

- ⚡ Identity and contact details of the data processor
- ⚡ Purpose and legal basis for processing the data
- ⚡ How the data will be processed
- ⚡ Who will be involved in processing the data
- ⚡ How long it will be kept
- ⚡ Their right to object to processing

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Organisations must provide data subjects with complete access to their personal data if requested

Data subjects have the right to access their personal data, so they can see what data is being held and what is being done with it. They can access this right by submitting a subject access request (SAR) which has to be responded to within one month and free of charge.

What has to be supplied:

- ❖ Confirmation that their personal data is being processed
- ❖ The purposes of the processing
- ❖ The categories of data being processed
- ❖ Who their data might be shared with
- ❖ How long their data will be stored
- ❖ The source of their data
- ❖ A copy of their data
- ❖ Their rights (to erasure, rectification)
- ❖ How automated decisions are made

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Organisations must provide data subjects with options to change their personal data without any restriction

Data subjects have the right to correct inaccurate personal data.

We have to erase or amend any inaccurate or incomplete data within one month of notice or two if the request is complex.

If personal data is shared with third parties, there is an obligation to ensure the information they hold is corrected.

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

If a data subject demands their personal data to be removed the organisation must comply immediately

An individual can request the deletion or removal of personal data and this has to be done when certain conditions are met.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.'

For when

- There is no compelling reason for its continued processing.
- The data subject withdraws consent.
- Their data was unlawfully processed.

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Data subjects can demand access to their personal data be restricted so the organisation can only access it for certain purposes

Individuals have the right to restrict processing when there is a dispute about the accuracy of their data.

When the data is restricted, it can be stored but not processed in any way.

We must hold just enough personal data to ensure that the restriction is maintained.

Third parties with whom the data has been shared must be informed.

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Data subjects must be given the option to transfer their personal data

Individuals can obtain and reuse their personal data for their own purposes.

The data must be provided in a format that is easily accessible or it has to be transmitted directly to another data controller.

Example

When an individual requests to switch utility supplier from one to another. The existing supplier is bound to provide all the information they hold on the data subject to the new provider (controller)

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

The data subject has the right to request the organisation stop processing

Individuals need to be informed as to their right to object when their data is collected.

If they object, processing needs to cease except for specific circumstances.

However, for direct marketing processing must stop immediately.

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Data subject have the right to demand the organisation stop processing their personal data if it is being used for other marketing activities

The GDPR gives individuals certain protections against the risk that a potentially damaging decision is made by a computer without the involvement of a human.

This extends to profiling and processing that on aspects such as health, behaviour or performance at work.

[BACK](#)[RETURN TO
INDIVIDUAL RIGHTS](#)[NEXT](#)

Learnings in this module:



Individual Rights

Individuals have a legal right to review the information you hold about them. If an individual makes an access request you have a month to supply the information – free of charge.



Right of Erasure

Individuals have the right to be forgotten. This means that you must erase their data if retaining it is not compliant with the GDPR or requested to do so by the individual.



Additional Rights

Individuals have the right to data portability, opting out of direct marketing and consenting to automated processing.

[BACK](#)[NEXT](#)

Module 4

Why Compliance Matters

[BACK](#)

[NEXT](#)

Module 4 Covers



Understanding a data breach



What to do in case of a data breach



How to reduce the risk of a data breach



Consequences of non-compliance



Summary

[BACK](#)

[NEXT](#)

A data breach occurs when someone gets unauthorised access to personal data

A personal data breach is whenever any personal data is lost, destroyed, corrupted or disclosed. These can include:

- ⚡ Access by an unauthorised third party
- ⚡ Deliberate or accidental action (or inaction) by a controller or processor
- ⚡ Sending personal data to an incorrect recipient
- ⚡ Devices containing personal data being lost or stolen
- ⚡ Alteration of personal data without permission
- ⚡ Loss of availability of personal data

[BACK](#)[NEXT](#)

Three steps need to be taken in the event of a data breach

If a personal data breach occurs an organisation needs to action the following:



Notify the ICO

You must notify the ICO within 24 hours of becoming aware of the breach.



Notify the customers

If the breach is likely to adversely affect the personal data or privacy of your customer, you need to notify them of the breach without unnecessary delay.



Record the details in the organisations breach log

You are obliged to keep a record of all personal data breaches in an inventory or log.

[BACK](#)[NEXT](#)

Improve IT security

The majority of data breaches are as a result of human error, poor internal systems and or lack of adequate IT security.

Here are some quick and easy ways you can implement to ensure security of personal data you hold.



Reduce human error

- ⚡ The majority of data breaches are as a result of human error



Improve internal systems and processes

- ⚡ Protect access to data
- ⚡ Don't let staff use their own devices



Strengthen your IT security

- ⚡ Strengthen password protection



Identify Phishing emails



Get protected with good anti-virus software

[BACK](#)[NEXT](#)

Significant consequences for failure to comply

Failure to comply through 'administrative failures' or 'personal data breaches' may result in:

- ✦ An investigation by the ICO with a range of range of corrective powers and sanctions
- ✦ Administrative fines

2%
Annual Global
Turnover

Tier 1 - for infringements of an organisations obligations - up to 10 million, or 2% annual global turnover – whichever is higher.

4%
Annual Global
Turnover

Tier 2 - for infringements of an individual's privacy rights up to €20 million, or 4% annual global turnover – whichever is higher.

- ✦ Liability of material and non-material damages from those affected
- ✦ Reputational damage and lack of trust

BACK

NEXT

Learnings in this module:



Understanding data breaches

A data breach occurs when someone gets unauthorised access to personal data. In the event of a personal data breach an organisation must: Report it to the ICO. Notify the individuals concerned. Record it internally.



Reducing the risk of data breaches

Understanding and improving IT security systems and processes will significantly reduce the likelihood of a data breach occurring.



Non-compliance

Can lead to: An investigation by the ICO, Significant fines, Compensation claims.
Reputational damage

[BACK](#)[NEXT](#)

Conclusion

[BACK](#)

[NEXT](#)

The training has given you:

- ⚡ A brief overview of the GDPR
- ⚡ The key principles underlying the GDPR
- ⚡ The legal rights of individuals to their personal data
- ⚡ Why compliance matters

Your next steps are to:

- ⚡ Understand data protection policies and procedures
- ⚡ Appreciate your role in protecting personal data
- ⚡ Identify when a task is within the scope of GDPR
- ⚡ Apply the GDPR principles to your work



END