Something like for us, a little bit cold, no problem, but just air-conditioned.

It will be a long day.

Anyway, we can start.

Just to sum up what we said last yesterday,

basically we talked about this important slide that was the individual rights.

We have to remember the individual rights that are fundamental in the GDPR.

And then we discussed about some cases.

One of the most important cases was caffeine-amidia cases.

Not because it was important caffeine-amidia, but because of Max Trance.

I hope that you have to Google it yesterday,

and you have to Google him in the next days.

And then we discussed about other important cases, but not so relevant.

And at the end, I briefly discussed about this case study that was in Muni.

It was the contact tracing app that we had in Italy.

But basically the Muni case was important because there was this distinction

between the symbolized data and analyzed data.

Now we have the first part of the lecture of the class

that will be more concentrated on the GDPR task.

It's not so amazing.

I have some case studies just to help you for the comprehension.

Again, like I told you last week, there are some things that will be useful for you

just to understand the GDPR, how it works in practice in GDPR.

How can you be compliant if you want to, for example,

make a startup and then need to know this kind of information.

Obviously, for the exam and for what we say,

generally the cause of the data protection lecture is not so connected.

But it's an important part of the course because my part was obviously

to present you the GDPR from a concrete way.

So I can describe to you the case study,

but I need also to explain to you how it works in practice,

how a company, how a data controller applies this kind of stuff.

So we can start with these four points.

That is basically the most important rule that is analyze what you collect and where.

Check if the time you store personal data is relevant,

inform your client how they can modify or delete their data,

and monitor who has access to personal data.

So these four important rules are basically the fundamental rules of the GDPR.

Because the first is the processing activity register.

Then there is the data retention and disposal policy.

And this is really important.

I repeat since the beginning, remember that less data you have, less risk you have.

Because if you delete data, you don't have any kind of risk.

So we will see in the last class when we discuss about data breach.

Then it's important to inform your clients, so the privacy policy.

I know that the privacy policy is something that makes us crazy

because nobody of us, nobody of me are able to read a privacy policy.

There is an interesting speech made by the Italian Data Protection Authority.

And in this speech it explains that when you wake up in the morning

and you have for example an Apple Watch and then you have an Alexa near to you,

and then perhaps you have a fridge that is a smart fridge.

This is a scenario that is not so possible to have these three devices when you wake up.

You have, and this is true, the privacy policy of Apple, Amazon and Samsung for the fridge

are basically you need 32 minutes to read all these three documents.

So just to give you an example, in a perfect scenario you have to wake up

and then you have to read 12 minutes the privacy policy of Alexa, Amazon,

then you have to take 10 minutes to read all the privacy policy of Apple

and then you need also 10 minutes to read the privacy policy of the Samsung fridge.

So if you want to use this device in a theoretical way you have to read all this information.

So you can understand that it's quite impossible because every day we install an app

and we don't have the time to read all this information.

That's why it's something that is important, but when we say inform the client,

inform the person, the physical person, the data subject,

you also have to use another important discipline that is now in Stanford in the United States,

that is legal design. What is legal design?

Legal design is the way to create legal information in a way that is comprehensible

for a person that is not a legal person.

We need to avoid dark patterns.

Do you know what is dark patterns?

Anybody of you knows what is dark patterns?

Okay, we'll show you a video that will explain you what is dark patterns.

You have to understand absolutely what is dark patterns

because we live in a dark patterns world.

So basically it's important that you have this third pillar that is the privacy policy,

but not the privacy policy that we have now that is a wall of text

and you are not able to understand and also you don't have the time to read all this information,

but we need to change the approach.

This is another story, but it's important for you to know.

And then obviously we need to monitor who has access to data.

Data protection means protection of data.

So you have to work on this direction to help the user

and help the data subject to protect his or her data.

This is an example of what is a processing activity register.

So when we talk about analyze what you collect, this is just an example.

You can use a lot of formats.

This for me is interesting.

It's the CNIL, that is the Data Protection Authority of France.

And you have the business branch, the name of business process, the owner process,

the functional description of processing, the purpose of processing,

the basis for processing, the type of processing, data and data subject used,

data subject categories, storage, retention period is important, disposal.

How can you delete this kind of data?

Original source, third party, name, data transfer, technology, description, and comments.

So you have to fill this form for any single data processing activity

if you want to comply with GDPR.

So this is in a certain sense a mess, but it's important

because when you do this kind of exercise, you start to understand

how much data you have and how can you manage this data.

It's really difficult to complete this register, especially if you fill all this information.

But when you have finished, you have a clear scenario of what is your data

in your company and your legal entity.

So basically the game is analyze what you collect and where.

Then you have obviously a task distribution,

and you have some players that are really, really important.

And then you have data controller, data processor,

general controller, data protection officer,

and all these players should distribute different tasks.

Data subject. Who is the data subject?

It's important to know this definition because I repeat every time since the beginning.

For me it's normal to have this kind of distinction,

but perhaps for you it's not the same.

So remember the data subject is an individual person

resident in the European Union and the subject of personal data.

You should also be a data subject, a physical person that is not a European Union citizen.

That's why it's important to remember that he is a resident in the European Union.

So also a simple domicile.

Some of you are not from the EU, but in this moment your domicile is in Europe.

So any member state should respect the GDPR for any person even if he is not a European citizen.

Then data controller is an institution, business or person that process personal data.

For example, e-commerce website or whatever.

Any legal entity.

And then we have data protection officer.

This is the most tricky figure that has been introduced with the GDPR.

The DPO is a person appointed by the data controller

that is responsible for overseeing data protection practices.

So basically you have this person that is involved to monitor,

to help the data controller to monitor the data processing activity.

Every single day I was in call when I arrived here with a person that is not so expert about data protection

and he told me that he wants to see if I want to participate in a tender

where there is the possibility to manage 87 companies as a data protection officer.

And I explained to this woman that basically it's impossible to be a data protection officer of 87 different legal entities

even if you are in a group because you need to have a lot of person that works on this kind of stuff.

What is important to understand is that there is no idea of how complex is data processing,

how complex is managing data.

That's why it's important to create a culture of data protection.

Because in the next future everything has passed through data and digital data.

So it's not a function that you say okay, but it's just a role.

So I say that you are DPO and then you don't have to do anything because there is a lot of activity.

And it's impossible for a physical person or also for a legal entity to manage 87 different legal entities

unless you are, for example, a big four or an important and enormous company.

But this is just to make an example of how complex the data protection officer activity is.

And then there is the data processor.

Data processor, we have already seen this kind of subject that could be a company,

an institution that process data on behalf of the controller.

So this is the classic example, Google, Facebook, and whatever.

But you don't have to think only about data processor like Google

because there is a lot of other data processor.

For example, if you give me your letter and then I have to just bring a letter from one place to another place,

I transport data.

Why I make this example of the letter?

Because also data protection always thinks that it's also connected to data,

but it's also connected with data also in a physical way.

So not only in a physical way.

So data processor is the subject that process data on behalf of the controller.

And then at the very end there is the data protection authority.

This is public institution monitoring implementation of the regulation in the specific U member county.

Then again these three distinctions, data controller, data processor, joint controller.

Well, data controller determines the terms that are proposed for which and the means by which personal data is processed.

So basically the data controller has the power to decide for what reason and for what purposes

the personal data is processed.

So for example, if your company organization decides why and how the personal data should be processed,

it's the data controller.

Again, the same definition, just that it's important.

The data processor is the natural or legal person or the authority agency

which processes personal data on behalf of the controller.

The controller decides, the data processor acts.

And then there is the joint controller.

When two or more data controllers jointly decide why and how to process personal data are collectively known as joint controllers.

Joint controller relationship arises more commonly than many people realize.

So there is a lot of situations where more data controller works together to become a joint controller.

So data subject, data controller, data protection officer, data processor, data authority.

And then again, the real stakeholder are data controller, data processor, joint controller.

Remember this point.

When we go to the data processor activity, the decision making power over the data processing is the criteria

for distinguishing between controller and processor.

Different level of control over data processing and different accountability and liability.

Quality of the data processor.

Data processor must provide sufficient guarantees to implement appropriate technical and organizational measure

in a such manner that processing will meet the requirement of the GDPR.

So there are contractual relationship between controller and processor, the article 28.

That regarding the subject matter, the natural proposes of the processing, the type of personal data and the obligation and right of the controller.

Why it's important definition of the data processor?

Because in any single problem that we normally have in data protection, the role of the data processor is crucial.

Normally any data breach is committed by the data processor.

So it's important that you choose the right data processor.

Because normally when you are a data controller, the most important thing is to save cost.

So in every single day when you go in the supermarket and you want to buy a beer or a coke, you try to find the best price normally.

This is the first option that you try to find.

But you have also to see the quality.

When you buy a coke, basically you have a certain guarantee of the coke.

When you ask to a person to manage your data, it's not like coke.

When we talk about AWS, we could agree or not agree or disagree, but AWS has a standard like a coke, like a certain kind of beer of quality.

And then you can have the sufficient guarantees because it's a service that is absolutely well known and has absolutely sufficient guarantees.

But at the same time, when you start to use other providers, other suppliers, you have to check if this supplier provides sufficient guarantees for the data processing.

So what is the main problem that we have in a practical sense?

And this is a case that happens in Italy, but that happens around the world in every single situation, is the lack of data processing agreement.

Because between the data controller and the data processor, so these two figures, there should be always a data processing agreement.

It is an agreement where you can define what are the tasks of the data processor.

So it's a contractual agreement, a contract between these two persons.

And normally there is a contract between the first entity and the second entity, but not a DPA, a data processing agreement.

It is something that is an addendum, it's something that you have to add to the contract.

And in this case, GSG was the data controller and it was in a contractual relation with the processor Verizon, who provided geolocation devices.

The controller installed this device to track the vehicle delivering goods on its behalf.

These vehicles were not directly owned by the controller, but rather by a third company in which the controller outsourced certain devices.

The data subject was the driver, employed by this third company, and he had no direct contractual relationship with the controller.

No controller-processor agreement existed between GSG and Verizon.

And the Italian DPA finds GSG for 5,000 euros.

So basically it's important to understand that it's absolutely an obligation.

The contract on the basis of Article 28 of GDPR, if you want to add this information, but it's not important.

It's important that the fact that you should know that there should be a contract. Why?

Because you need to know in advance what are the potential sufficient guarantees, again, if you see here.

The provider must provide sufficient guarantees to implement appropriate technical and organizational measures.

If you have a contract and it's a data processing agreement, so it's connected with the data,

you have a certain insurance that the provider guarantees a certain kind of protection.

But if you don't have this contract, you cannot demonstrate that you were accountable and you know this kind of information.

And then you have the sub-processor, because the supply chain, it's really important.

When we think of the data processor, we think just of the first level.

But then there is a second level that is absolutely important.

The second level is the sub-processor, because a data processor normally could use also a sub-processor.

Also when we think of Amazon, we have to think that AWS has a lot of data sub-processor.

The processor of the processor, this is the definition in a certain sense.

And the processor, again, can engage other processors with prior specific or general written authorization of the controller.

When you make this kind of agreement with the data controller, you have to remember that you have to list all the data protection,

sorry, all the data processors.

And if you change your data processor, you need to have a written authorization of the controller.

And this is really important.

The same obligation is set out in the contract or other legal act between the controller and the processor.

And guarantees to implement, obviously, appropriate technical organizational measure.

And then the initial processor remains fully liable to the controller for the performance of the sub-processor's obligation.

So it's boring, I understand, but it's important that you follow the supply chain.

The supply chain is really important, because if you say, okay, my processor is a good processor,

and you don't check who is the sub-processor, so the processor of the processor,

perhaps the processor is really reliable, but this processor used another processor that is not reliable.

So you need to check, if you are the data controller, obviously, all the processors.

Not only the first one, but also the sub-processor.

And then we have this case, again, lack of authorization to engage a data processor.

In this case, a web application provider who entered an agreement with a group of hospitals

to create the application for collecting and managing employees' whistleblowing reports.

Do you know what is whistleblowing?

Okay, whistleblowing is the opportunity that we have now in a lot of countries,

not only Europe, but the United States, and I know there is also in South America.

There is an obligation for this kind of, for the data controller and for the entity

to have the power to make an anonymous report to the data controller, to the legal entity.

So for example, if I am an employee and I have some problem,

and I see that my colleague commits a crime or commits something that is not ethical,

I can make a whistleblowing so I can write the report.

And this report should be anonymous, and nobody can know who I am,

but I have the opportunity to denounce, to explain to my employer that there is a crime that has been committed.

Then, obviously, I can also say about sexual harassment or any kind of unethical

and illegal activity that are committed in a company.

So this is the whistleblowing rules that we have around the world.

So we were discussing about this instrument, and sorry,

an instrument that contains a lot of confidential information,

because in whistleblowing reports, basically I make reports about legal activity,

not ethical activity, anyway, something that is really confidential.

So ISWEB contracted the company C-WEB for hosting the whistleblowing application.

ISWEB didn't ask the prior of the internationalization from the controller for engaging a super data processor,

and did not formalize its processor-subprocessor relationship with C-WEB.

So ISWEB claimed that the object of its contract with the hospital was only the provision of technological infrastructure,

but anyway, the Italian authority didn't agree with the obligation to find a processor for €40,000.

Why? Because the processor appointed a new subprocessor,

but the processor didn't advise the data controller.

So it's important also to have this chain that should be really clear and transparent.

So anyway, you change your subprocessor and you are a data processor,

you need to have the authorization of the data controller,

because the data controller is at the top of the line.

Just to anticipate one point, you see here that you have a data controller that is on the center,

and then you have a data subject, and then you have here a data processor.

It's not complete, this chart, because here you have a subprocessor.

So you should have a direct relation between data controller, data processor, and subprocessor,

and all these two are connected with the data controller.

So we were discussing about lack of authorization of the data processor,

and then we discussed about joint controller, Article 26.

Two or more controllers jointly determine the purposes and means of processing,

form an agreement between joint controllers,

determine respective responsibility and obligation in particular

as regards the exercising of the rights of the data subject

and their duties to provide information to the data subject.

The data subject may exercise his or her rights in respect of and against each of the controllers.

So I tried to explain this that could be a little bit complex,

even if you read the first line, it's pretty clear.

Joint controllers happen when two or more controllers jointly determine

the purposes and means of processing.

So for example, you have two companies that start a partnership,

and they want to organize an event here in Politecnico.

And so, again, automotive companies always use this example.

So Audi and Mercedes decided to organize an event to give you the opportunity

for all the students to try the new electric car of Audi and Mercedes.

So there is this opportunity.

And then all the data that are collected during this event

of the person that wants to try the car, and obviously if you want to try the car,

you have to give the data to the company, are shared between Audi and Mercedes.

And in this case, there is obviously a joint controller agreement

because they have the same purpose and they determine together jointly the same purposes.

So when there are some data controllers, some legal entities that together decided

to make a certain processing, they are called joint controllers.

Why is it important, the joint controllership, in a practical sense?

Not for the example that I mentioned, but when you think of a bank,

when you think of Google, when you think of an incredible organization,

there are many, many entities.

For example, Banca Sella, that is a little bank here in Turin,

but is quite important for the Italian system, has more than 34, 35 legal entities.

And there are a lot of services, perhaps the Italian guys use Hype,

that is one service that is jointly made by Illimiti and Banca Sella,

that have two companies, so they have decided these two banks,

Illimiti and Banca Sella, to offer a service that is quite easy as an app to exchange money.

So if you use this app, your data are viewed by Banca Sella and Illimiti.

And then Banca Sella needs also, but not because it's bad things,

but just to give you better services, to know that you have, for example,

a bank account with Hype, but then you have also a bank account with Banca Patrimoni,

that is another bank.

And then if you can make a joint controller agreement,

that all this data could be connected, and then you can offer services

that is better for the client, for the user, for the data subject.

This means also for Google.

When you have Google and YouTube, for example, are different companies,

but all the information that are present in Google are viewed also in YouTube.

So when you see a video, the information that you have put on Google

could be seen also by YouTube, and this gives you better services.

Perhaps you say, oh wow, uncontrolled, and in a certain sense you are right.

When you say uncontrolled, the right word should be I'm profiled,

because it's true that this kind of activity of profiling

would be used for economic purposes to use your data to make money.

And this is one of the purposes of Google.

But at the same time, it's to give you a better experience in the hub.

And when you are in YouTube, it's absolutely true

that all the information that you have put on Google could help you.

Think when you are in a Google map, and also you have the same activity,

because Google remembers a lot of information about your search

and then helps you to find immediately a certain place.

So there is some services that are connected.

You can see in a bad way, and it's true also, and I agree with you,

that is how I am profiled.

They make money with my data, too.

But it's also true that the joint controllership,

so to put together different entities,

gives the opportunity to give you better services.

That's why it's important the joint controller agreement.

But it's important that you know that there is a joint controller agreement.

It's important that the data subject, from a native perspective,

knows very well who are the players that manage your data.

So that's why it's important to have a data processing,

sorry, joint controller agreement,

where it's absolutely clear who is the player.

And then we have these Jehovah cases in 2017,

where Jehovah Witness community collected personal data

during the door-to-door activities,

including names and addresses of personal known to them

without their knowledge or their consent.

Both the members of the community were involved in the activities

that were aimed at engaging in preaching,

keeping records about preachers,

and distributing community publications.

They were forbidden from doing so

unless the legal requirements for processing were satisfied.

The court held that a religious community is a controller

jointly with its members who engage in preaching

for the processing of personal data

carried out by the letter in the context of door-to-door preaching,

organized, coordinated, and encouraged by that community.

Without it being necessary, that community has access to those data

or to establish that community has given its members written guidelines

or instructions in relation to the data processing.

So I don't want to be so much complex,

but the basic information is that all these legal entities,

even if they are religious,

legal entities should be linked with a joint controller agreement.

Then, what are the digital relations?

I have already explained to you what are the relations.

So you have the data controller in the middle,

and you have data processor, sub-processor,

and then you have potentially another controller in this scenario.

So if you have two controllers,

there is a joint controllership agreement,

and they are joint controllers.

And at the very end, we need to help data subjects.

We need to protect data subjects that are really, really important.

Okay.

We can go to the accountability principle again.

This is a principle, really important, accountability.

And then I already mentioned about this principle.

Now it's a little bit better explained,

as I mentioned to you in the last lecture.

But it was really important to remember that accountability

is the way to demonstrate the fact that you have been complied

with the data protection law.

With that general principle, the obligation of the data controller,

the security measure, and the risk management,

that means reporting obligation, data breach, business continuity,

disaster recovery, data protection impact assessment,

code of conduct, certification, and seals, and a lot of stuff.

We obviously not go in detail of all this kind of activity.

Sorry, guys.

And then we have the data protection strategy,

mapping data flows and processing activity,

mapping task resolution, assessing potential risk,

defining procedural and technical measure,

increase accountability, define a data protection strategy,

identifying weaknesses and priorities,

and then you should have a data protection officer and a team of experts.

I don't want to go, obviously, in detail of this because, again,

I already, the important issues are here.

That is this part.

Remember this four pillar.

Analyze what you collect and where.

Check if the time you store personal data is relevant.

If not, remove data retention and disposal.

Inform your CHI policy and monitor

who has access to personal data.

These are the four pillars.

Obviously, if you want to implement these four pillars,

you have to go also through this general principle and this strategy.

But anyway, it's more important to go and analyze case by case

this information.

Again, the important things for the exam is the four pillars.

Then accountability case.

In this case, Enel Energy is an important Italian energy provider,

so not only Italian but also international provider.

The Italian authority received hundreds of reports from users

who received unwanted promotional phone calls.

The phone calls were often made by partner companies,

not by Enel itself.

Citizen reported a persistent and disturbing sense of interference

in the sphere of privacy due to this practice,

which are often not only invasive but also particularly aggressive.

The authority established a violation of Article 5 and 25

for not having taken effective action against and due promotional

contests made in its name by exercising its duties of accountability

and privacy by design.

And then Article 5.2.4.5 being to provide evidence of compliance

with data protection legislation.

This is important.

The evidence of compliance, then we come back to this point,

in the case of unsolicited promotional communication

by a business partner.

And then Article 5 and Article 24 for failing to control the activities

of its business partners, including through appropriate technical

and organizational measure.

Why it's important this word in these cases?

Because since the first lecture, since the first class,

you have seen that there is no only one answer

when we talk about data protection.

Also when we discussed together, we had different opinion.

I remember last Tuesday when we discussed about the consent

and the data monetization.

And if you want, if you remember,

Lituania and the girls tell me about the fact that you,

in a certain sense, agrees with the newspaper solution,

if I remember well.

And you, if I remember well, a different opinion.

And there is no person that is right or wrong.

Because it's something that is already based on the principle

of accountability.

That's why you can, in a certain sense,

it makes crazy the situation.

But I think that there is a reason why there is no only one

answer.

Because the technology is something that we cannot keep.

We cannot have a clear clue of what will happen,

a clear strategy of what will happen with technology

in the next year.

But also in the next minutes, we know every one of you probably

know the Moore's law.

But now we are all, we have finished the Moore's law.

We are in a situation, especially with artificial intelligence,

think of the chart of GPT, that it's not predictable

what will happen.

So how can you fix a law that tells you what is right or not?

Obviously, there are some principles,

and these principles are really important.

The fact that we should protect personal data,

special categories of data, judicial data.

These are the general principles.

But then when you go case by case,

it's not possible to say you have to respect all these rules

because the rules change with the time.

And the time is really, really, really brief.

There is no possibility.

Think of the cybersecurity issue.

Any fix, any bug that you have, and then you make a fix,

and then every single day you have other vulnerability,

and then you have other way to attack a system.

So we cannot say in the first, in the older,

in the former law of data protection,

we had one thing that was the 10 rules,

I call it 10 rules about cybersecurity.

It was the password should be more than eight characters

with some special characters and all this stuff.

I think that now it's absolutely stupid to say

that the password should be just of eight characters,

more than eight characters,

because it's something that we cannot protect.

You should have a double factor authentication measure.

But then probably in the next five years,

also the double factor authentication

cannot be the only, the right solution.

We will find other way to make a secure authentication.

So how can we write a law that impose something

that we know that in a couple of years

cannot be the right system?

So that's why there is the accountability,

because we don't know how to protect data.

We know now probably how to protect data,

but what I say today, probably tomorrow is not correct.

And this is the most important lesson

that I wanted to learn in this course,

that data ethics, again, data ethics,

it's really important because if you work with ethics,

you have a common language,

even if you have different culture,

and we need to respect different culture to protect data.

It's something that we need to underline.

And then the second point is not only data ethics,

it's accountability.

And accountability is provide evidence of compliance.

You should provide this kind of evidence.

It's important because even if you make a mistake,

if you explain why you make this mistake,

and there is some evidence that you make a reasoning

about this mistake, and at the very end you do,

if you did this mistake in good faith,

probably you will not be sanctioned,

or the sanction should be really, really a little sanction.

So basically this is the accountability case

and accountability principle.

You should provide evidence of compliance.

This is what the legislator asked

and the data protection authority verified.

And we say the role of the most important person

in the accountability principle is the data protection officer

because the role of the data protection officer

is to be between the data controller and the data subject,

and he needs to work or she needs to work

with the data controller.

So you have, for example, in a data breach,

I have a TPO of some company,

and then the data protection authority called me

and asked me how the company managed this situation.

And so I have to be really transparent

with the data protection authority.

But at the same time, my fees are paid by the data controller,

so I should be also a consultant for the data controller.

So it's something that perhaps for you it's difficult to understand,

but this image explains very well how it's complex

to be the person that is in the middle

between the data protection authority and the data subject.

And he has to help or she has to help the data controller

to respect the data subject's rights.

But at the same time, the data controller wants to use the data

and is not so, or she is not so interested

to protect the data of the data subject

because any kind, any form of protection means money

because you have to spend money if you want to protect data.

So that's why it's important this kind of role.

The data protection officer is mandatory

for public authorities or bodies,

and then for core activities consisting in processing operations

which require regular and systematic monitoring of data subjects

on large scale of data,

and whose core activities consist of processing on large scale data

of special categories of data or personal data

related to criminal conviction or offenses.

So the data protection officer is not compulsory.

You can also decide not to have a data protection officer,

but if you process special categories of data

or you do any kind of systematic monitoring of data,

you should have this kind of role in your company.

What are the qualities of the data protection officer?

Expertise in a national and European data protection laws

and practices including an in-depth understanding of GDPR,

understanding of the processing operation carried out,

understanding of information technology and data security,

knowledge of the business sector and the organization,

and ability to promote the data protection culture with the organization.

So when we talk about the GDPR since the beginning,

in 2014-15, the law was approved in 2016,

then was entered in force in 2018,

all the person always say, sorry,

that the data protection officer should be an IT and data science guy.

And then what happened that all the data protection officer are lawyer.

This is a big, big problem that we have,

and I hope that we will change in the next future this role

and you start to become a data protection officer.

Why? Because it's true that in a certain sense there is a lack

when you are a data scientist that is a lack of knowledge of law

that are really important in the GDPR scenario.

But it's also true that one of the most important qualities

is understanding of the processing operation carried out.

What happened in the normal situation?

That you have a lot of piece of paper,

because we are lawyers so we love to write a lot of piece of paper,

and then we start to produce all this documentation

regarding the activity of a company.

But then when the data authorities ask to a data protection officer,

okay, explain me how this company works in terms of security.

And then if you ask to an attorney and say,

oh, yes, the company has a lot of antiviruses.

Yes, okay, I imagine that they have antiviruses,

but can you go a little bit in depth of what is the way

to put the CDC in a safety situation, in a secure way, the company?

And then there is no knowledge about cybersecurity principles

that are fundamental in data protection.

And then you say, okay, you are not prepared on cybersecurity side.

Please explain me what is the core business of this activity

when we talk about data.

And then there is no accurate answer,

because an attorney cannot know how data works,

how is the data flow in a company.

And this is fundamental if you want to protect data.

Because if you want to respect the principle that I told you before,

so you want to inform, for example, the user how the data is managed.

You want to make a correct data retention policy.

So you want to delete data.

You need to know how the data works.

And it's not the job of a legal person,

but it's a job of a more IT person.

So that's why, at the beginning, the Article 37 was deemed,

has been thought, for not a legal person.

Then it happened that we have more lawyers rather than IT.

My dream is to have half and half,

because it's important to have a cooperation

between these two different competence,

because on one side it's important the compliance,

but the compliance without understanding what is the matter,

what is the data flow, it does not make any sense.

It's just a piece of paper that is perfect,

but it's just a theoretical rule

without any kind of concrete applicability

if you don't know how it works.

Then another role of the data protection officer is the independence.

So provide the resources necessary

to carry out the data protection officer task

and access to personal data and processing operations,

and to maintain ease or expert knowledge.

No instruction by the data controller or data processor

regarding the exercise of DBO tasks.

No dismissal or penalty by the controller

for the performance of DBO tasks.

No conflict of interest with potential and other tasks,

and DBOs are not personally responsible for non-compliance.

So it's simple, but it's important.

Obviously the DBO should be absolutely independent.

Then we go through some examples, some cases.

So the Spanish data protection authority

imposed a fine of 25,000 euro for Glovo

for non-compliance of its duty to appoint a data protection officer.

So the defendant asked for a statement not to be included

among the men that were appointed,

but Glovo also stated despite the fact

that it had an internal data protection board,

but the Spanish data protection authority

didn't accept this obligation

and therefore started the sanction procedure.

Glovo stated that in 2009

it had formally appointed the data protection officer,

but it had decided not to make this appointment public until 2020

because the board and the legal department of Glovo

had been already developing such action effectively.

But anyway, the Spanish authority

ultimately imposed the sanction of 25,000 euro.

Now the sanctions are a little bit more important.

In 2019, in 2020, sorry,

the sanction was a little bit less for COVID-19 reasons

and for the application that was just a couple of years.

But basically, the basic issue is that Glovo is obviously

a company that should have a data protection officer.

Do you know why Glovo has an obligation to have a DPO?

Think of the definition.

I think Dr. DeSantis said that Glovo is a public authority.

I don't think so.

But Glovo's activity consists of processing

on a large scale of special categories of data.

Why special categories of data?

Because your preferences on food could be special categories of data.

Why?

Because perhaps you have some allergies

and this is a factor that could have an impact on your data.

So we can make Glovo is able theoretically

to profile all the person that has some personal disease

or some religious disease because some kind of food

are specific for certain religious practices

also in certain periods of time.

So you can have a lot of information

if you know what the people eat.

So it could be a special category of data.

I know that for you it's quite crazy,

but again, I repeat that you have a lot of information.

I had a direct experience of that.

So Glovo, then there was also other cases

with the Conservatory of Music in Rome

for processing and disclosing personal data

found on a misplaced USB drive

without the legal basis and violation of the proposals

and for appointing the DPO in a position of conflict of interest.

So in this case, the DPA underlined the fact that

the principal was the controller's data processing officer.

So it's not possible to have the data protection officer

that is the same person of the legal representative,

the principal, the owner of the company,

because obviously the owner of the company

cannot control himself, so there is a clear situation

of conflict of interest.

And then we have another case,

the German Federal Data Protection Authority

imposed a fine of 10,000 euro on rapid data

for the non-compliance of its duty

to appoint a data protection officer.

In Germany, a DPO should be accompanied by a company

where at least 20 employees work with personal data.

Indeed, in Germany there is a more strict application

of the data protection law.

In fact, Article 37 says that

the Member States National Law may impose the appointment

in cases other than those listed under Article 37.

And in Germany they decided to have more DPO

because they understood that the role of DPO

is absolutely important.

So last slide, and then we go to make a short break.

Launch of coordinating enforcement on the role

of data protection officer.

I put this information just for you,

but it's not important, just for your curiosity,

because it's really great news.

The Data Protection Board,

the European Data Protection Board has kicked it on

and coordinated enforcement action

through the 26th Data Protection Authority

will take part in the sort of designation

and position of data protection officer.

So that's why it's an important way that we have now

to implement, to reinforce a new role

that is quite crazy rules, as I explained you before,

because it's a role that is in the middle

between data controller and data subject.

And it's important that we have a guideline,

a precise guideline to explain better what is the rule.

So I finish this part and then we can have a break until 5.30.