Pridatect

European Study on Data Protection in the Health Sector 2020.

Contents

01. Current situation

The coronavirus pandemic has had various effects on the healthcare sector with regards to data protection. Organisations have implemented previously inconceivable measures in order to try to continue with business as usual as best they can, without putting patients or staff at risk. But as the use of healthcare apps and mobile location data is on the rise, so is the potential for attack and exploitation.

Healthcare & Special Category Data

For those operating in the healthcare sector, special care must be taken when collecting, storing and using personal data. Medical records are considered special category data under article 9 of GDPR legislation, meaning (as the term suggests), special care has to be taken by data controllers when treating this extra sensitive information.

Before going any further into what to do and how to do it, the very first step you must take is to ensure you have the lawful basis to process data in the first place. The factors to be considered are as follows:

- **Consent** *(given by the individual)*
- **Contract** *(processing is necessary to fulfil contractual obligations to individual)*
- **Legal obligation** *(processing is necessary in order to comply with legal obligations)*
- **Vital interests** *(to protect someone's life)*
- **Public task** *(processing is necessary in to protect the public interest)*
- **Legitimate interests** *(legitimate interest of you or a third party unless there is a good reason to protect the individual's personal data).*

In addition to lawful basis, when treating special category data, the organisation must also have an Art. 9 condition for processing.

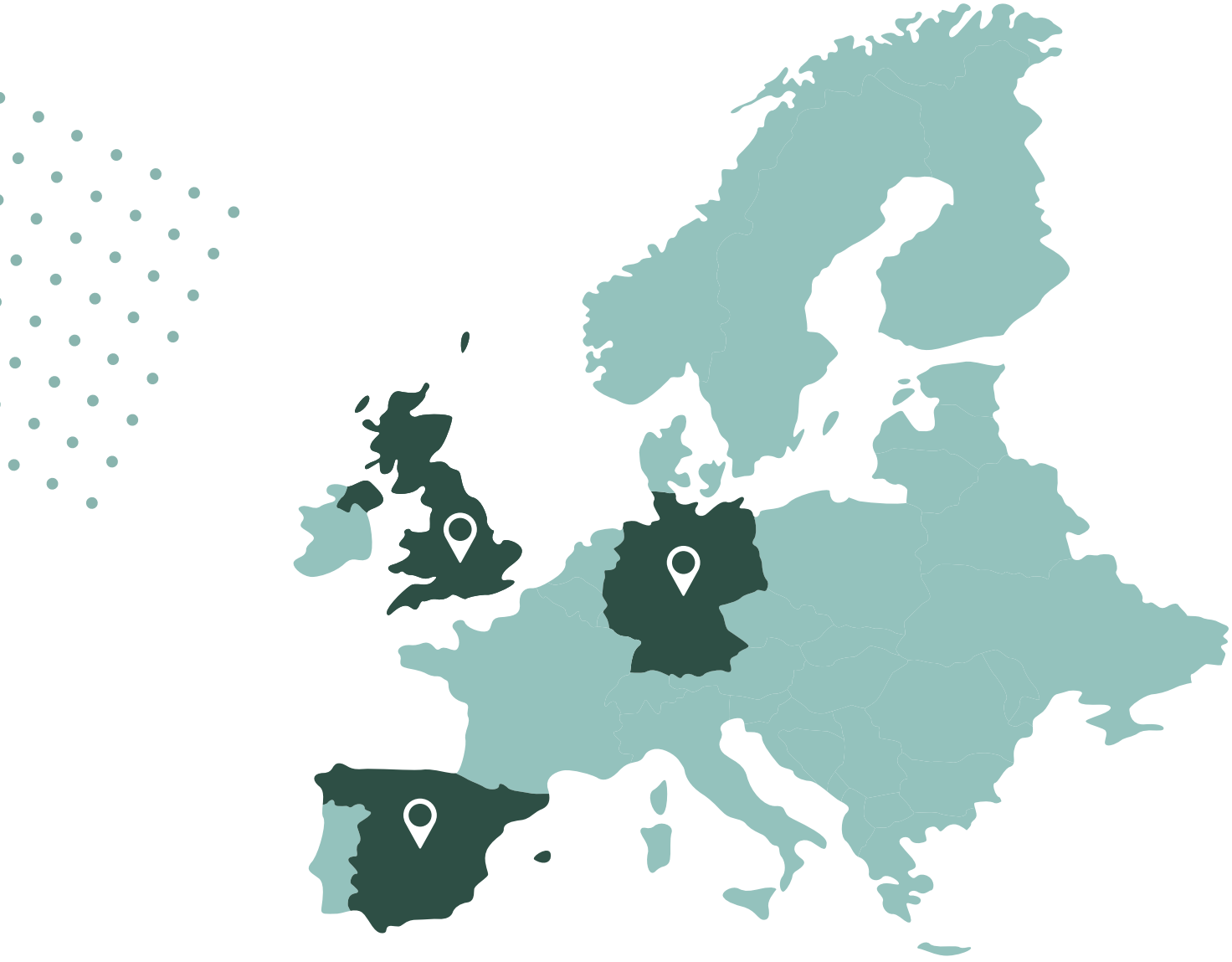
Once it's been established you have the legal right to process data, **we can move onto how to do this correctly, and whether companies in the healthcare sector are doing so.**

We've conducted a study to assess GDPR compliance in the health sector, to see how aware companies are of what needs to be done to ensure compliance, so let's dive in.

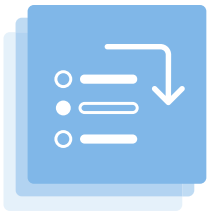
02. Methodology

In order to establish the contemporary compliance landscape and to provide good practices for organisations, in May 2020 **we surveyed CEOs and managers of 300 organisations in the health and pharmaceutical sector in the UK, Spain and Germany** in order to complete this study.

We received 100 responses from each country and will focus primarily on **results from the UK.**



03. What are health sector organisations doing about data protection?



A. Perception of compliance:

We analyzed just how important data protection is to companies in the health industry.

B. Collection and processing of personal data:

We examined the level of compliance with GDPR with regards to informing patients and clients or establishing the necessary consent and confidentiality agreements when sharing data.

C. Security policies and measures implemented in organizations:

We found out whether or not organisations are using the recommended guidelines and protocols to carry out processes that ensure the protection of personal and health data with which they work.

A. Perception of compliance:

Question 1

On a scale of 1 to 5, how important is data protection to your organisation?

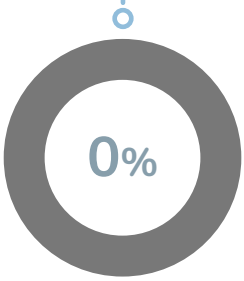
With the changes/ digitalization in healthcare, doctors, hospitals, pharmaceutical companies, and many other providers of health-related services are increasingly forced to deal with data protection and security issues. **GDPR classifies health data as particularly sensitive data, and this makes it inevitable that they require special protection.**

Are organisations aware of this?

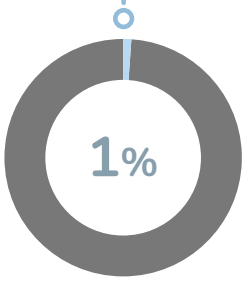
The results of our survey clearly show that although only none of the organisations say data protection isn't important at all, only **89% of health sector organisations consider it to be "very important"** despite the fact that fines for non-compliance can be crippling.

As we can see from the results, there is a general similarity on a European level, with around three-quarters of respondents stating that data protection is very important to their organisation, although it is markedly higher in the case of the UK. That covers what companies say but as the saying goes, the proof is in the pudding, so let's move on and see what these organisations actually do.

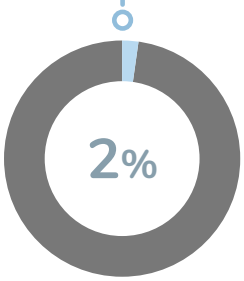
Not at all important



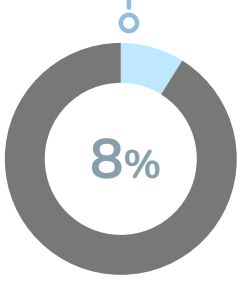
Slightly Important



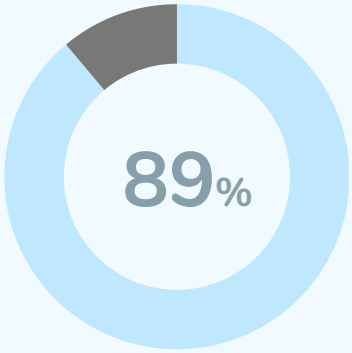
Important



Fairly Important



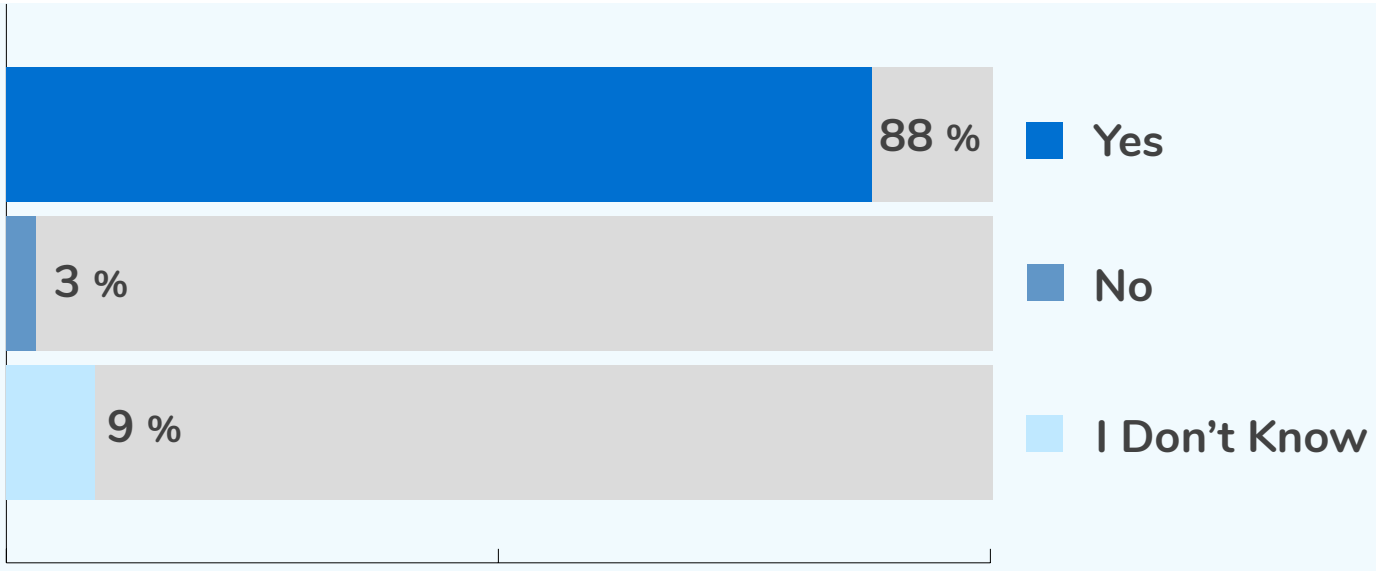
Very important



A. Perception of compliance:

Question 2

Does your organisation meet the require-ments to comply with GDPR?



A series of steps must be taken to ensure compliance, which include having a DPO if necessary, conducting risk assessments, impact assessments, identifying possible safety gaps and having both preventive measures and a protocol to manage them.

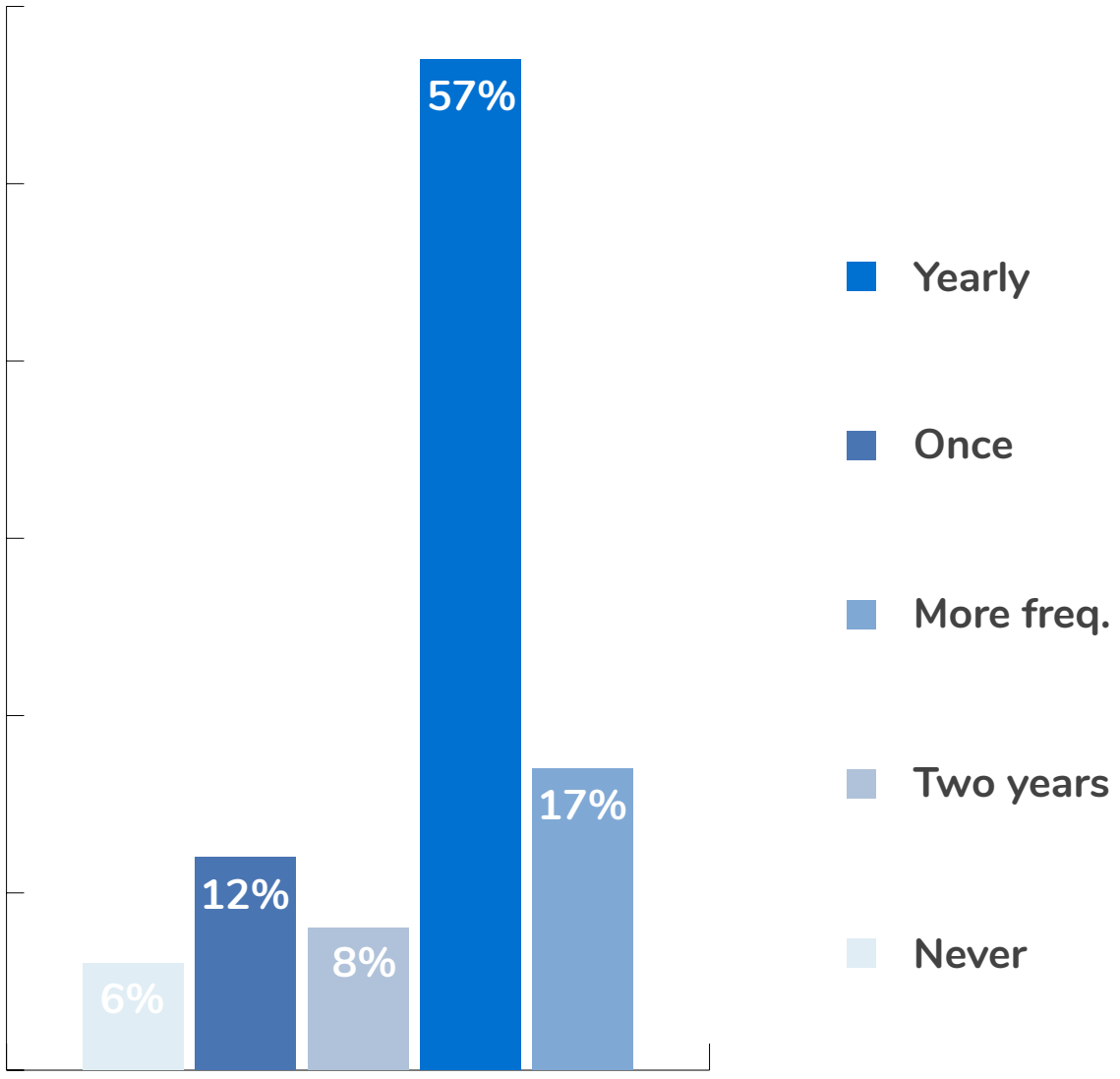
If you have a website or services offered via apps, information sent by email, etc., you must also comply with all requirements regarding privacy policies, cookies, etc. For this reason, we wanted to know whether or not health organisations believe that they meet all the requirements to comply with GDPR.

The results of our survey show that 88% of the respondents in the UK claim that they do meet the criteria for GDPR compliance. This is comparable with the rest of Europe, with around 80% responding positively. However, **it is more alarming to see that 3% in the UK readily admit that they do not meet all the requirements for compliance.**

A. Perception of compliance:

Question 3

How often does your organisation conduct data protection training for employees?



Although companies are gradually getting to grips with the importance of data protection, in practice the issue is somewhat neglected at times: it is usually the employees who have to work to comply with data protection requirements in their daily activities.

GDPR does not include any direct training requirements for employees, but compliance with GDPR obligations is almost unattainable without them. We can see through the graphic above that data protection is generally perceived (and treated) similarly, across the board.

6% percent of UK health organisations surveyed do not conduct any data protection training for their employees, similarly to Europe as a whole, with around 11% of those surveyed never providing training to employees. **Contrast that with how important companies said data protection was to them earlier, and we start to see that what they say doesn't exactly line up with their actions.**

The evidence from the UK is more in line however, with the majority of companies claiming that data protection is important to them, 74% providing training either frequently or annually.

One of our in-house data protection experts had this to say on the matter of regular training for employees.

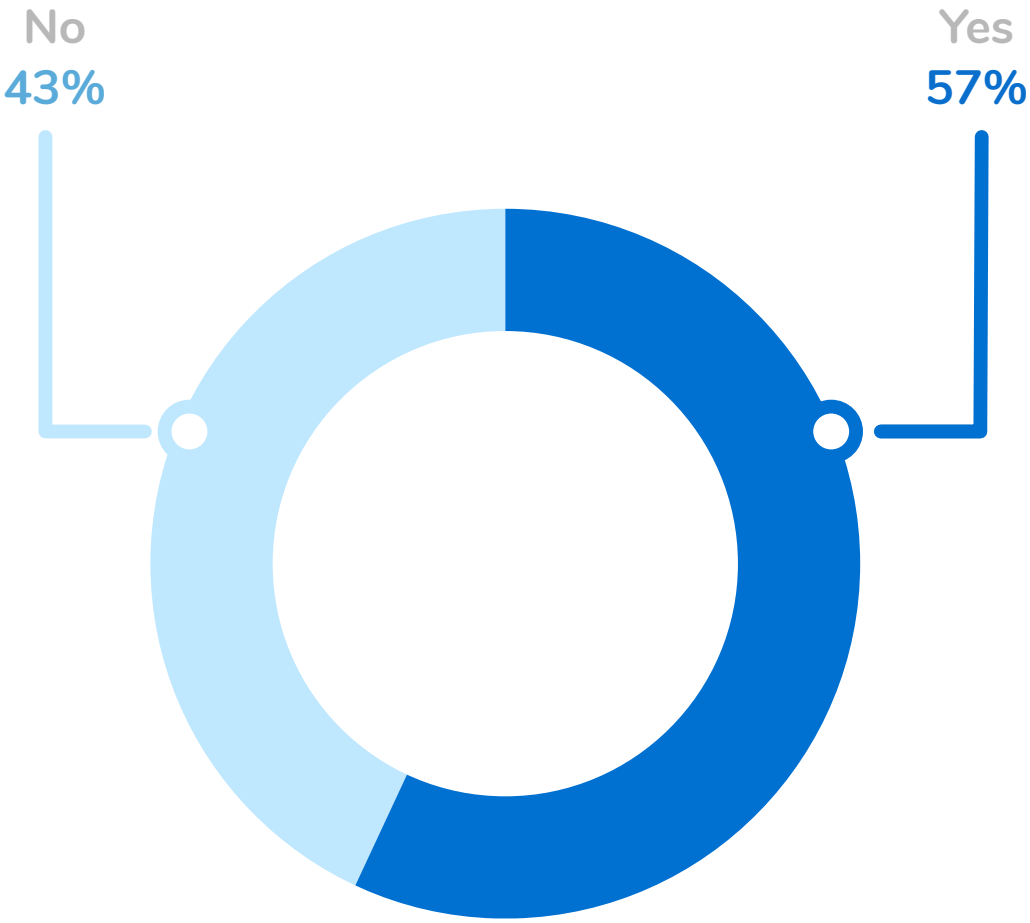
"Only 17% of organisations guarantee recurrent training for their employees in the area of data protection. **There is no doubt that more investment is needed in this organisational measure**, *as it is considered the most effective in mitigating risks".*

Eva Estevez | DPO at Pridatect, lawyer specialized in data protection

B. Collection and processing of personal data:

Question 4

Do your customers/patients ask about data protection?



Approximately three-fifths of patients or customers in the health sector actively ask companies or institutions about the protection of their data. This high level of interest reaffirms the importance of handling the data in the right way and awareness that neglecting data protection can damage the reputation of the company and the business itself.

Just over half those surveyed said that their customers are asking about data protection, which seems low when we look at the data on a European level, with around 70% of respondents professing that clients do ask about data protection.

European results

No
34%

Yes
66%

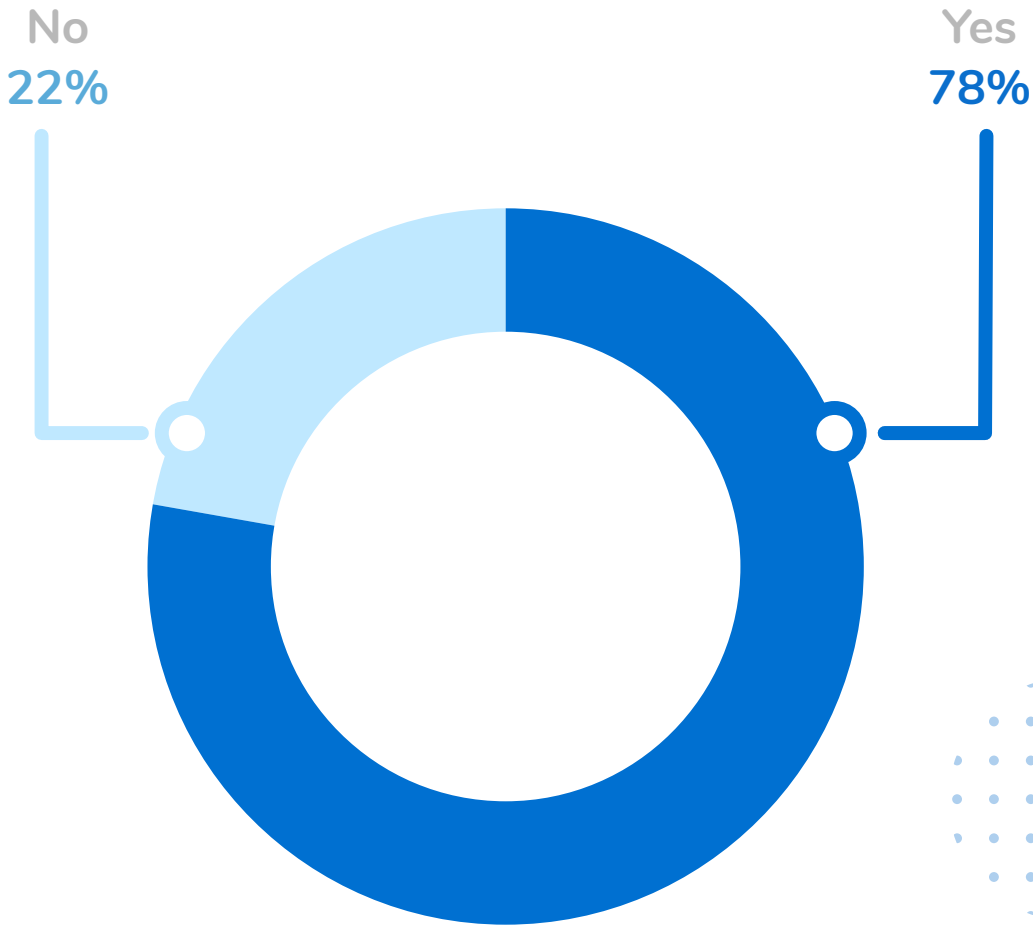
"57% of respondents say that their patients/clients ask about data protection, *demonstrating a significant level of interest; which makes data protection compliance not only an obligation but also an indication of quality and trust for customers".*

Andrea González Fuentes
| Legal Advisor at Pridatect

B. Collection and processing of personal data:

Question 5

Do your customers/patients ask about the purpose of collecting their personal information?



Around three-quarters of companies surveyed said that patients were interested in why their data was collected. A key component of GDPR is an individual's right to be informed about the collection and use of their personal data. Here we can see that the vast majority of patients (around three-quarters) want to know why their data is being collected.

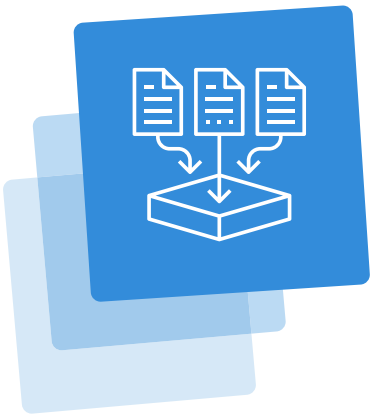
Not content with simply handing over their personal information, **patients want to know why you need it and what you will be doing with this information,** this is something covered in the next question, 'does your organisation inform patients/clients about how their personal data is being treated?'.

Continuing on with the initial question, the need for data collection in healthcare is obvious, to provide the best possible care for the patient, but this must be communicated at the time it is collected.

The following information (known as privacy information) must be provided to individuals within a reasonable period of the data being obtained:

- **Purpose** for processing personal data.
- **Retention** period.
- **Who** data will be shared with.

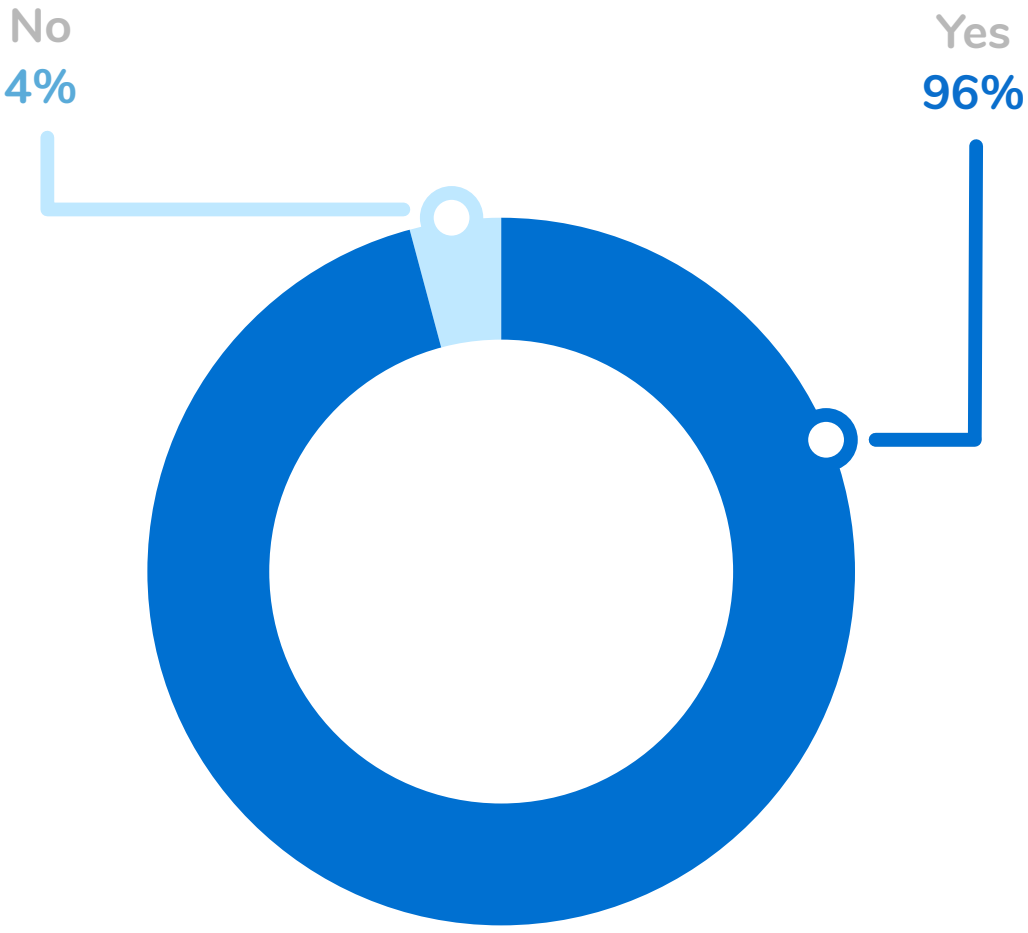
Best practice here is to make these things clear at the point of initial data collection so the user is able to make a decision as to informed consent.



B. Collection and processing of personal data:

Question 6

Does your organisation inform patients/ clients about how their personal data is being treated?



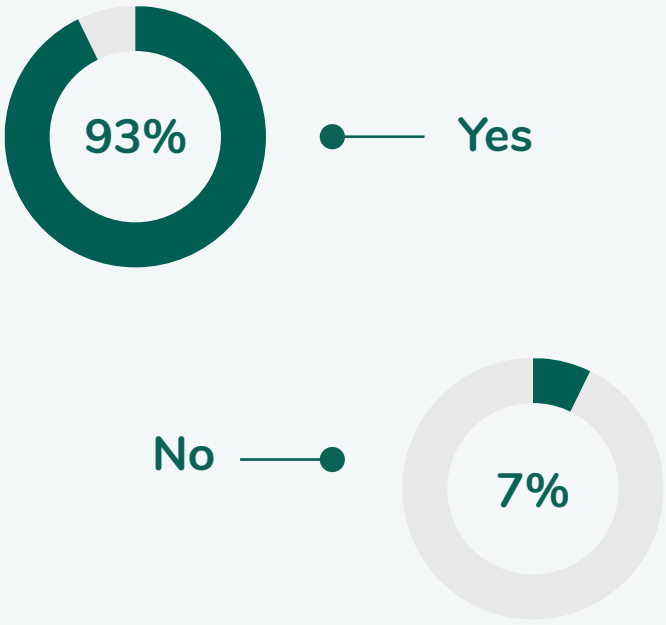
Leading on from the last question, and how the vast majority of patients/clients want to know how their data is treated, and that GDPR came into effect more than 2 years ago, it is interesting that around **4% of respondents simply fail to inform clients about how their personal data is treated.**

This basic requirement not being met by a substantial portion of those surveyed is worrying. Informing clients about data treatment is fairly straight forward, failure to comply in this aspect leads to sanctions.

Aside from the fines that lack of compliance leads to, there is also consumer trust, it's well known by now that the trust between consumers and organisations that is garnered through **secure data storage provides a clear competitive advantage.**

We need to establish what we mean by personal data so we're all on the same page, so let's take a look at the guidance provided by the ICO.

Compared with data on a European level, around 7% do not inform clients about how their personal data is being treated.



Personal data is information that relates to an identified or identifiable individual. Meaning name, number or IP address for example.

We can see that despite the importance of communicating how personal data is treated to individuals, approximately 7% of respondents readily admit that they just don't do it. If data is used to communicate with an individual, or is disclosed to another party, **this must be disclosed.**

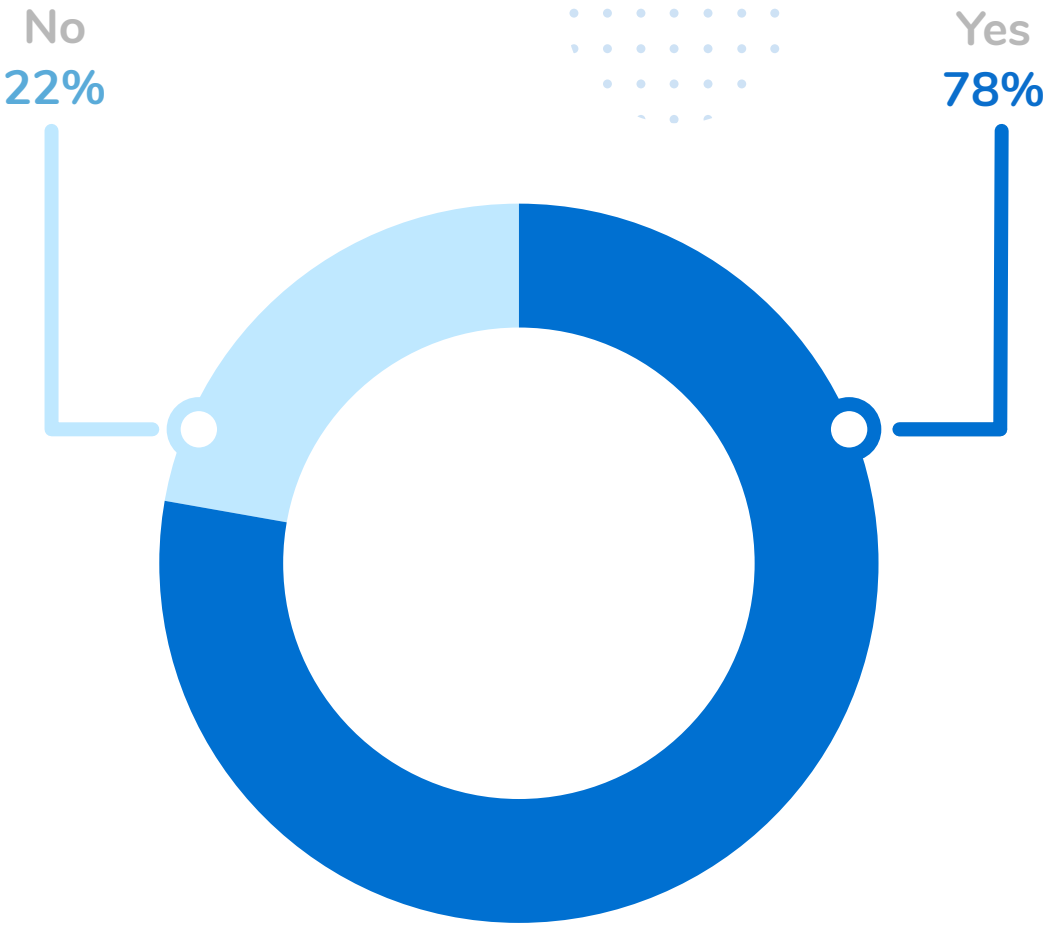
"Organisations are increasingly aware of the processing of personal data of the stakeholders with whom they interact (customers, suppliers, workers, etc.). *Likewise, 94% of organisations guarantee the duty of information in the processing of data".*

Eva Estevez | DPO at Pridatect, lawyer specialized in data protection

B. Collection and processing of personal data:

Question 7

Does your organisation obtain consent for data processing?



What type of personal data can a company collect?

Name, surname, age, address or indicators of user needs according to the products they purchase. **Looking at organisations in the health sector we find more sensitive data, such as test results, medical history, any diseases they suffer from or medication they take.**

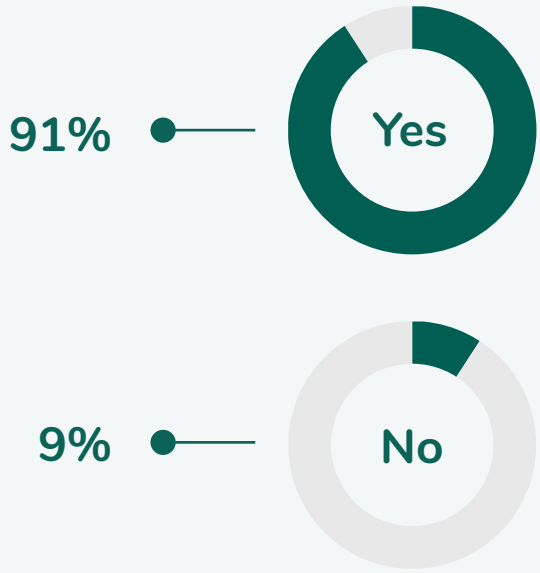
Around three-quarters of companies surveyed across Europe obtain user consent, but that means a quarter of companies, don't do so when necessary.

It seems that data collection is almost unavoidable, and this has been demonstrated in this study.

Most of the people surveyed stated categorically that they do collect personal data, with up to 91% of them answering that they do not ask for or use any personal data from customers, employees or suppliers.

The result makes it unquestionable that there is a need to have a protocol in place when dealing with this data and to adapt to the GDPR to ensure its protection.

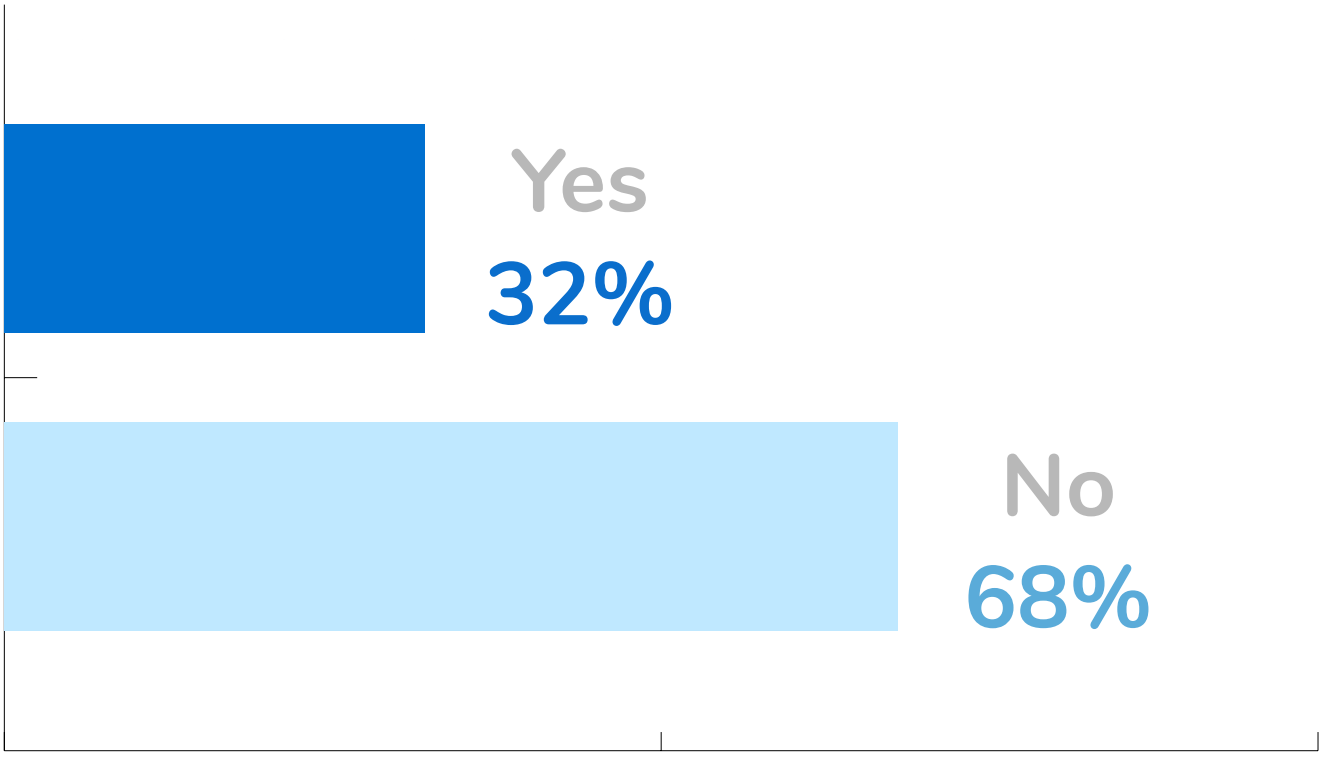
European results



B. Collection and processing of personal data:

Question 8

Does your organisation share personal data with third parties (Software, providers, business partners, accountants, etc.?



Despite the onus on companies to protect user data, with just under a third of companies sharing data with third-parties. 32% of respondents indicate that they do share data with third parties, while the figures on a European level are slightly lower at 31%. Despite the fact that more companies treat their data internally, inter-company data traffic is quite common.

Sometimes, data sharing agreements can be made, where one company gives another the freedom to use specific data. **This would inevitably require specific and unambiguous consent set out in a legal contract.**

Although sharing data with third parties is not an extremely common practice, **it may be necessary in some cases to seek the assistance of a third party for a specific need.** For example, a health centre that has to send a patient's tests to a laboratory for analysis, or a dental clinic that has to send a patient's data and measurements for the production of dental materials.

Here again, it is necessary to specify (in a contract) the obligations of the company that will process this data, and the company would need to select a data processor. These are assumptions that, although they are not part of the day-to-day life in your organisation, it is necessary to take them into account and to foresee how this relationship would be legally established in order to avoid an inappropriate use of the data or that they run some risk.

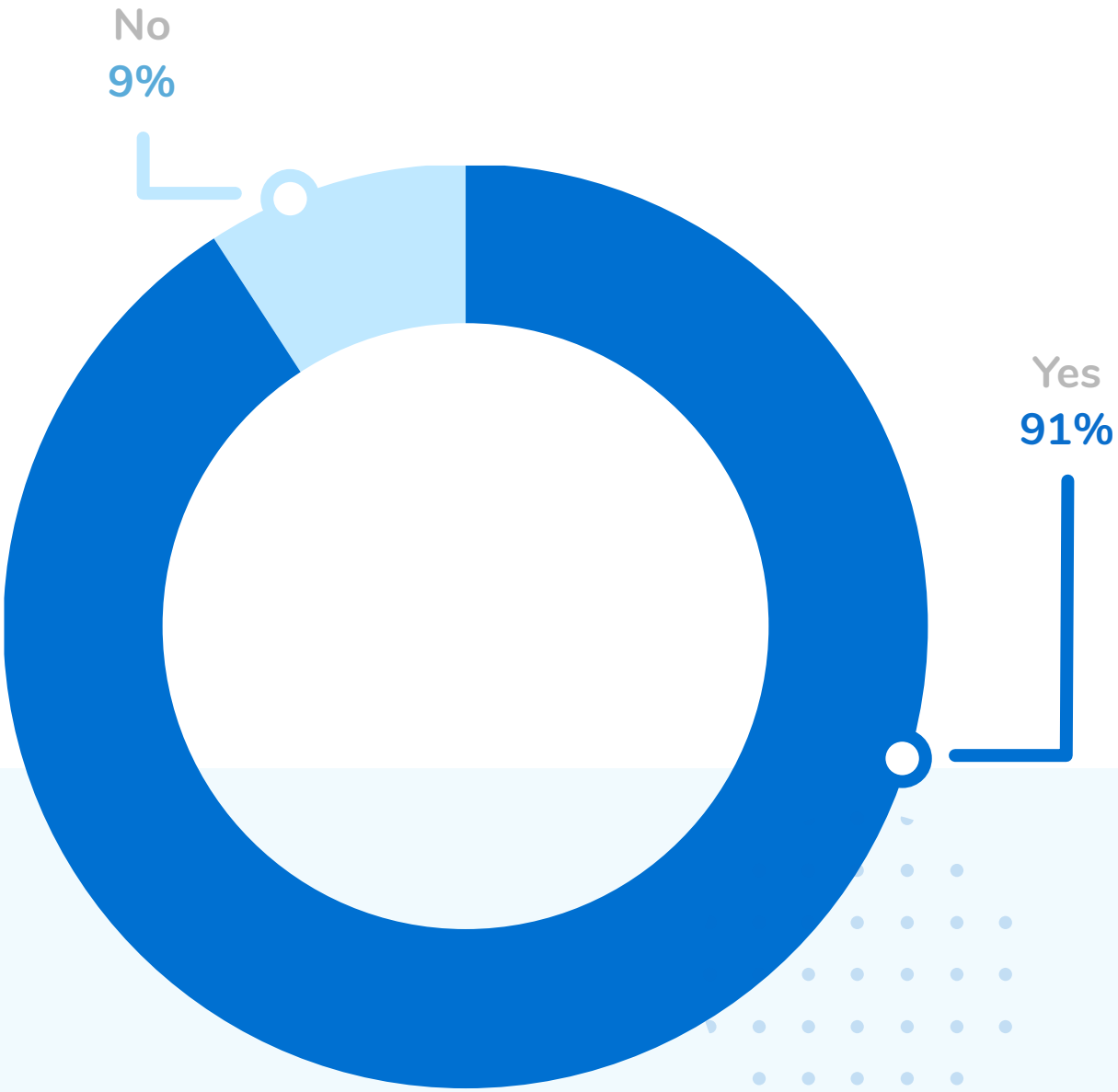
B. Collection and processing of personal data:

Question 9

Do you have a signed confidentiality agreement with third parties?

Over 91% of respondents do have a confidentiality agreement with third parties, and are therefore setting out the obligations and limitations beforehand. However, almost 9% of respondents do not stipulate terms in a contract, providing leeway to third-parties to treat data how they wish.

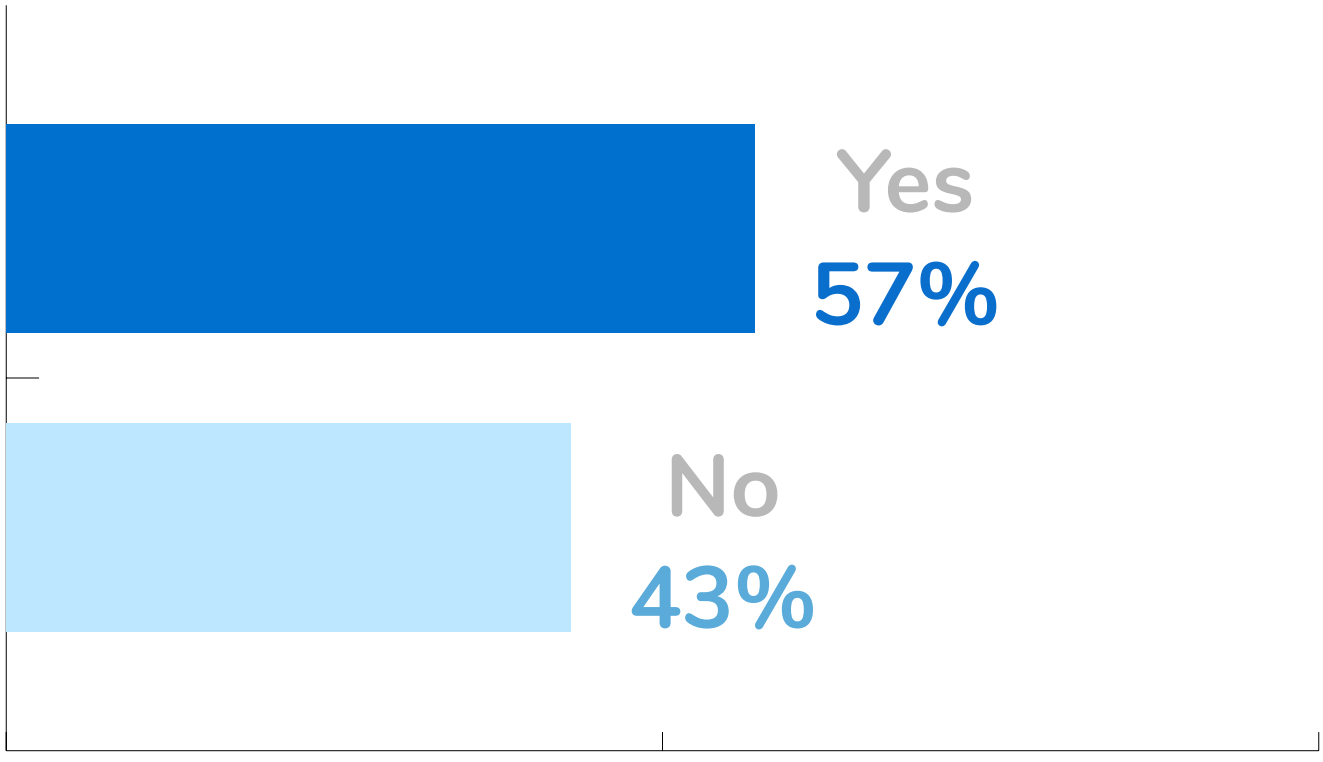
It is vital to establish in writing, and taking into account legal requirements, the obligation for the company to which the data is being lent to respect confidentiality and not to use that information for purposes other than those stipulated in the contract.



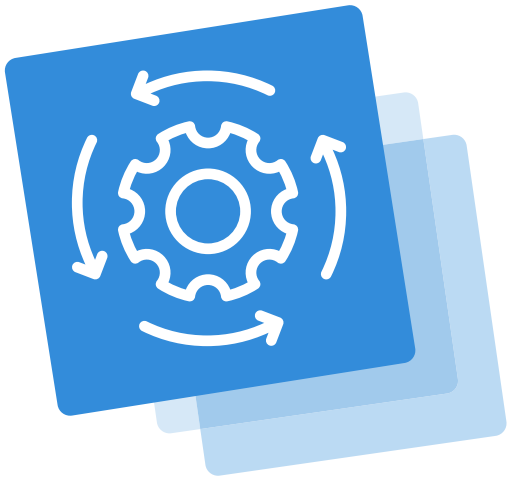
C. Security policies and measures implemented in organisations:

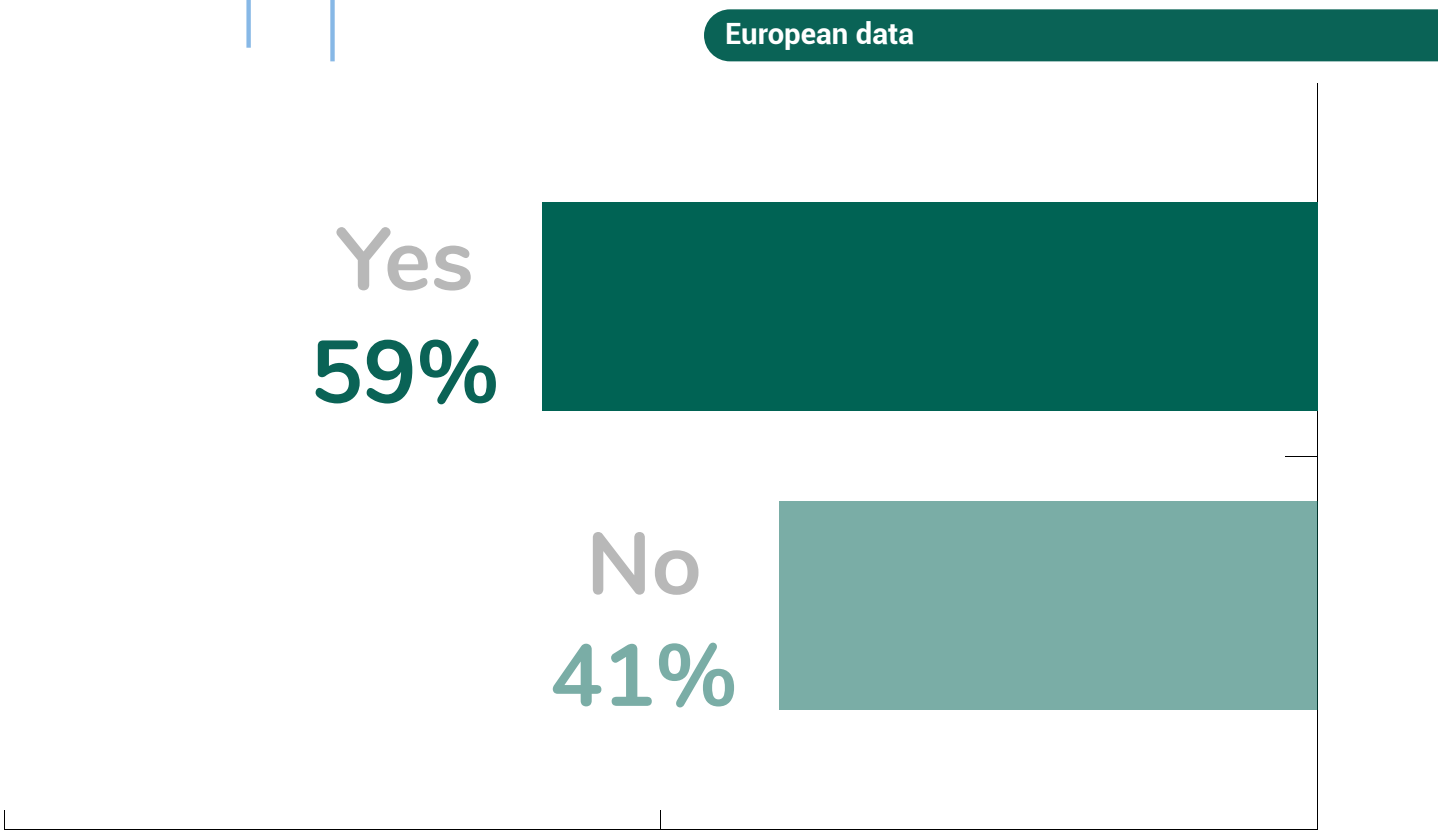
Question 10

Have you incorporated any software solution that processes health data into your organisation in the last 12 months?



57% of healthcare companies in the UK have implemented new software solutions that process health data in the last 12 months, just a bit less than Europe, with 59% of respondents answering in the affirmative.

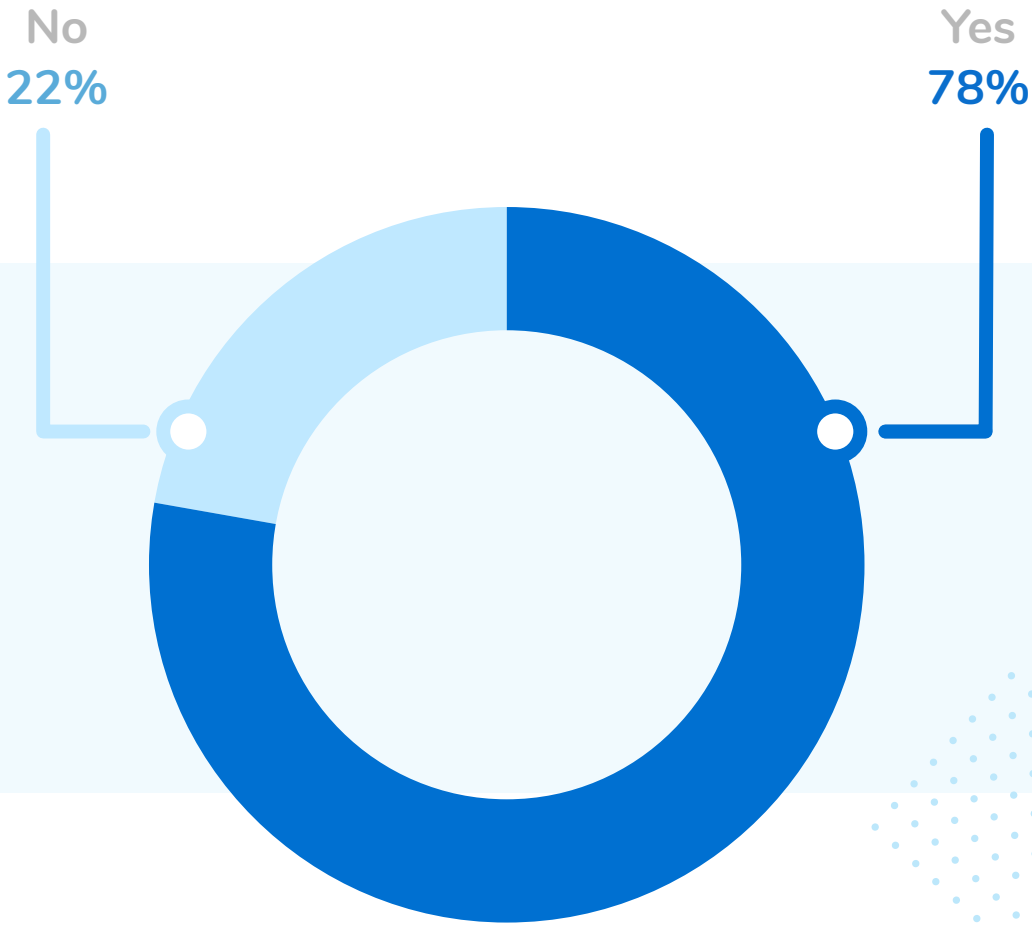




C. Security policies and measures implemented in organisations:

Question 11

Does your organisation have a DPO (Data Protection Officer)?



We can see that from this question alone, 22% of the UK companies surveyed are not compliant with the legislation, despite clear guidelines that they must have one appointed. There are similar figures from Europe as a whole, with approximately a quarter of those surveyed not having an appointed DPO.

This is a failure to achieve compliance, and will leave these organisations open to attack, and the resulting fines from failing to prevent this. Why? Without an appointed DPO, they're fumbling around in the dark, hoping they don't come under attack, rather than taking steps to ensure stability when they do come under attack.

Having a DPO is vitally important when it comes to compliance, the person who fulfils this role helps to demonstrate compliance to the relevant authority and plays a huge role in something the ICO is extremely hot on, accountability.

Accountability is an important topic because some organisations try to say 'we didn't know' or as incredible as it sounds, more than one organisation thought they were 'too small to have to comply'.

The DPO can be an existing team member, but should be an expert in data protection. Tasks involved include advising the data controller (you) of obligations, compliance monitoring, and to be the first point of contact for the ICO.

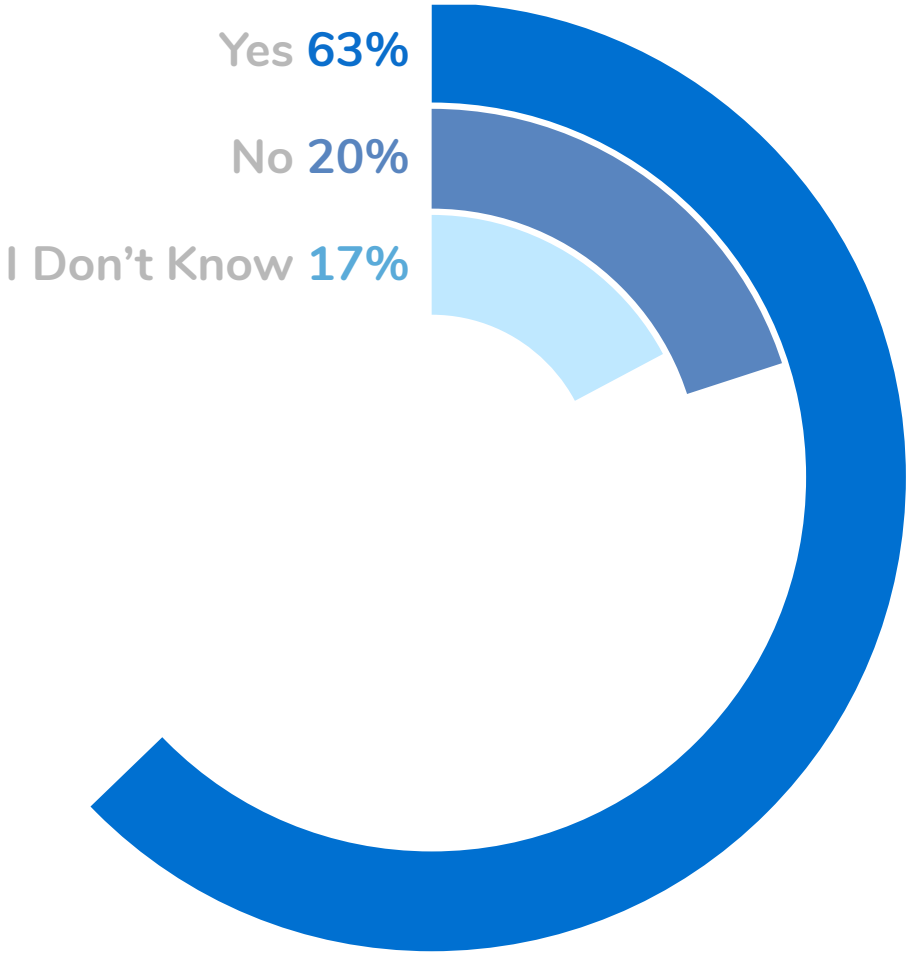
GDPR has been in effect for 2 years and we can see that at least 22% are not fulfilling this criteria of compliance. The importance of a DPO can also be evidenced when we say that compliance is ongoing, it isn't simply a one off. A DPO assists in ensuring your processes are in line with the latest regulations/ guidelines but also demonstrates the companies willingness, and efforts to achieve compliance.

Just take a look at a case from Hamburg, Germany, a €51,000 fine of a German subsidiary of Facebook. The supervisory authority described this fine as a 'warning', sounds like an expensive warning to us! The reason for this fine? **The company did not have an appointed Data Protection Officer.**

C. Security policies and measures implemented in organisations:

Question 12

Has your organisation conducted a PIA (Privacy Impact Assessment)?



One of the key steps to ensuring data protection in a company is the Impact Assessment. A health professional, a centre or a company that works with sensitive data related to the health of its patients or clients, has to know the extent of the risks it would have to take on, and the damage that could be caused if a security breach were to occur or if this data was not treated correctly.

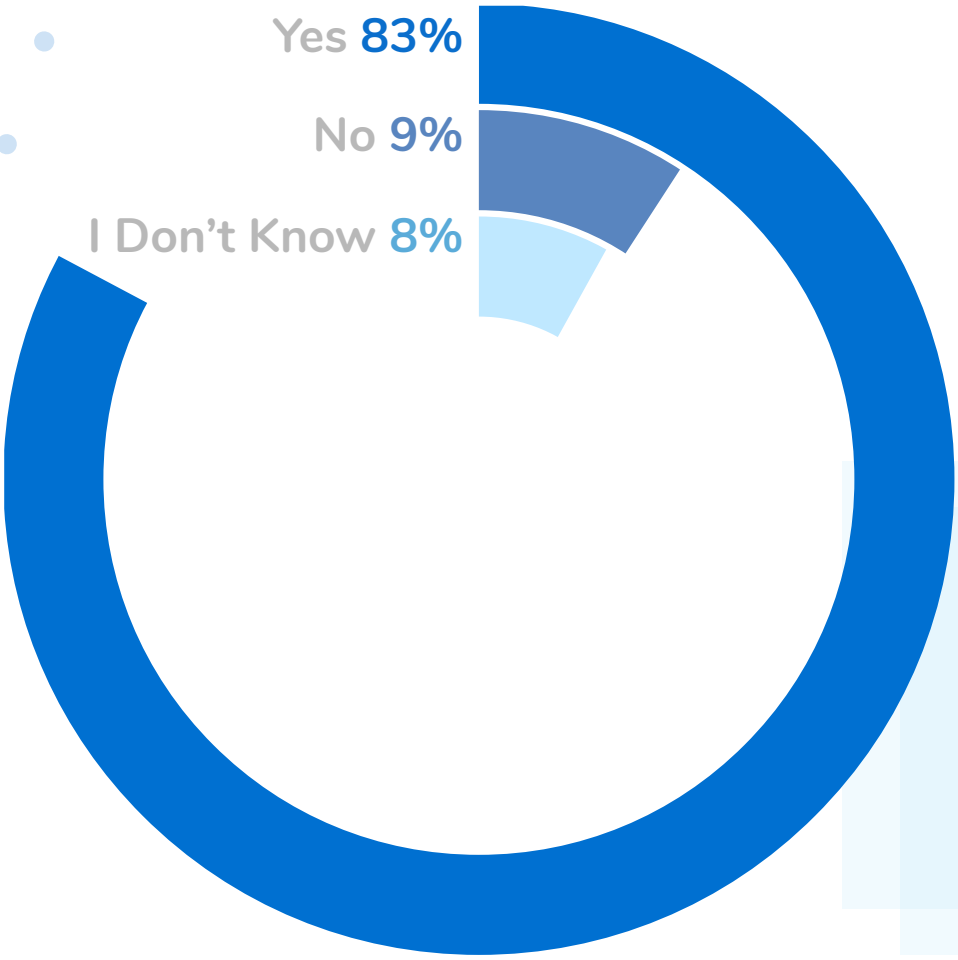
In this study we wanted to know how many companies in the health sector had carried out an Impact Assessment, and **63% of companies responded positively, which suggests that there is evidence of what an Impact Assessment can mean when it comes to establishing the necessary measures.** There are similar figures on a European level as around 60% of the companies surveyed said they had conducted a PIA.

Interestingly, around 20% of companies replied that they didn't know the answer, could this be tied to how many haven't appointed a DPO?

C. Security policies and measures implemented in organisations:

Question 13

Do you keep an updated record of data processing activities?



The chasm between the results we got from the UK (83%) and the rest of Europe contrast strongly, where two-thirds of the companies surveyed update records of data processing activities.

Much like GDPR compliance, updating your record of processing activities is an on-going activity. The recommendation from the ICO is to treat the record as a living document, reflecting the current situation

The record must be kept up to date with the following activities:

- **All parties involved in data processing** (controller, processors, representative etc)
- **Categories of data processed**
- **Purpose of processing**
- **How long data will be retained**
- **The technical and organisational security measures** (TOMS) **implemented** (when possible).

> **Only 83% indicated that they keep an updated inventory of processing activities. However, this obligation affects almost everyone who processes personal data.** *A supervisory authority will always ask you for the processing register first when auditing the company. It should therefore be the backbone of the data protection framework of any company."*

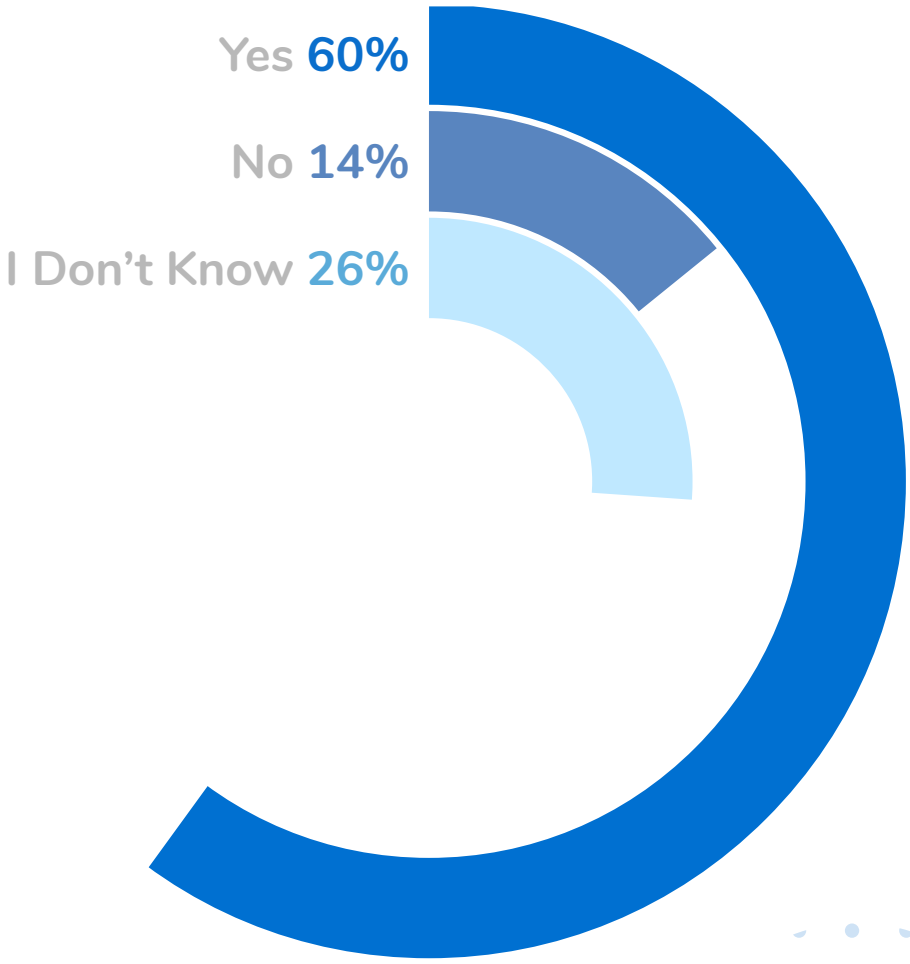
Lisa Hofmann | Chief of Legal Operations, Pridatect

There is no 'update the record once a week', but it should be updated as any changes to processing are implemented. As to the 8% who answered that they 'don't know' if they keep an updated record of activities, it's very likely that they don't. It's a document that has to be kept up to date with current activities, so if you did it, you'd be able to answer in the affirmative. **Failure to comply with this aspect of GDPR, leads to possible fines up to 10 million euros or 4% of the company's total revenue for the previous year.**

C. Security policies and measures implemented in organisations:

Question 14

Have you defined the Technical and Organisational Measures in your organisation to mitigate the risks of each data processing activity and thus define security measures?

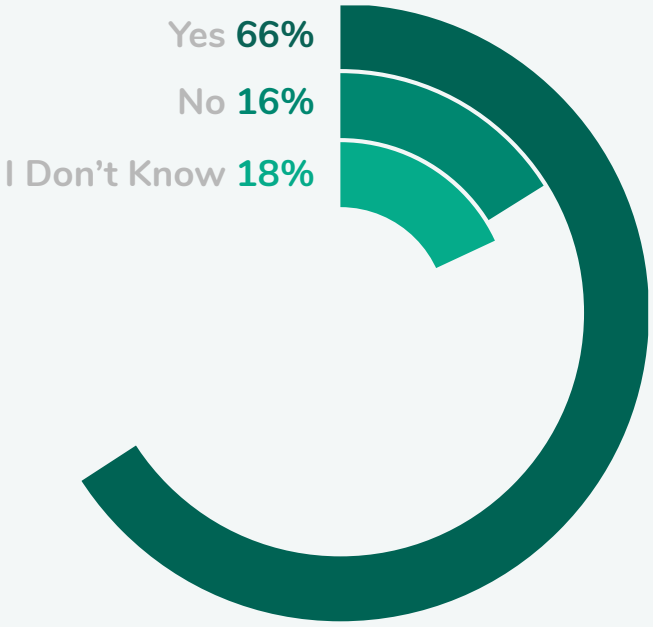


Taking technical and organisational measures (TOMS) helps to ensure the security of the data you are going to work with: potential risks are identified and measures are taken to avoid them.

60% of respondents say they do take them, but we found that 14% do not do so, and 26% answer "I don't know", implying that they are unaware of this practice or that they are not aware that it has been carried out in their workplace.

Taking technical and organisational measures is something imposed by **Article 32 of the GDPR**. It is necessary to demonstrate that the necessary measures have been taken so as not to breach regulations, in other words, to ensure that everything possible has been done not to put personal data at risk.

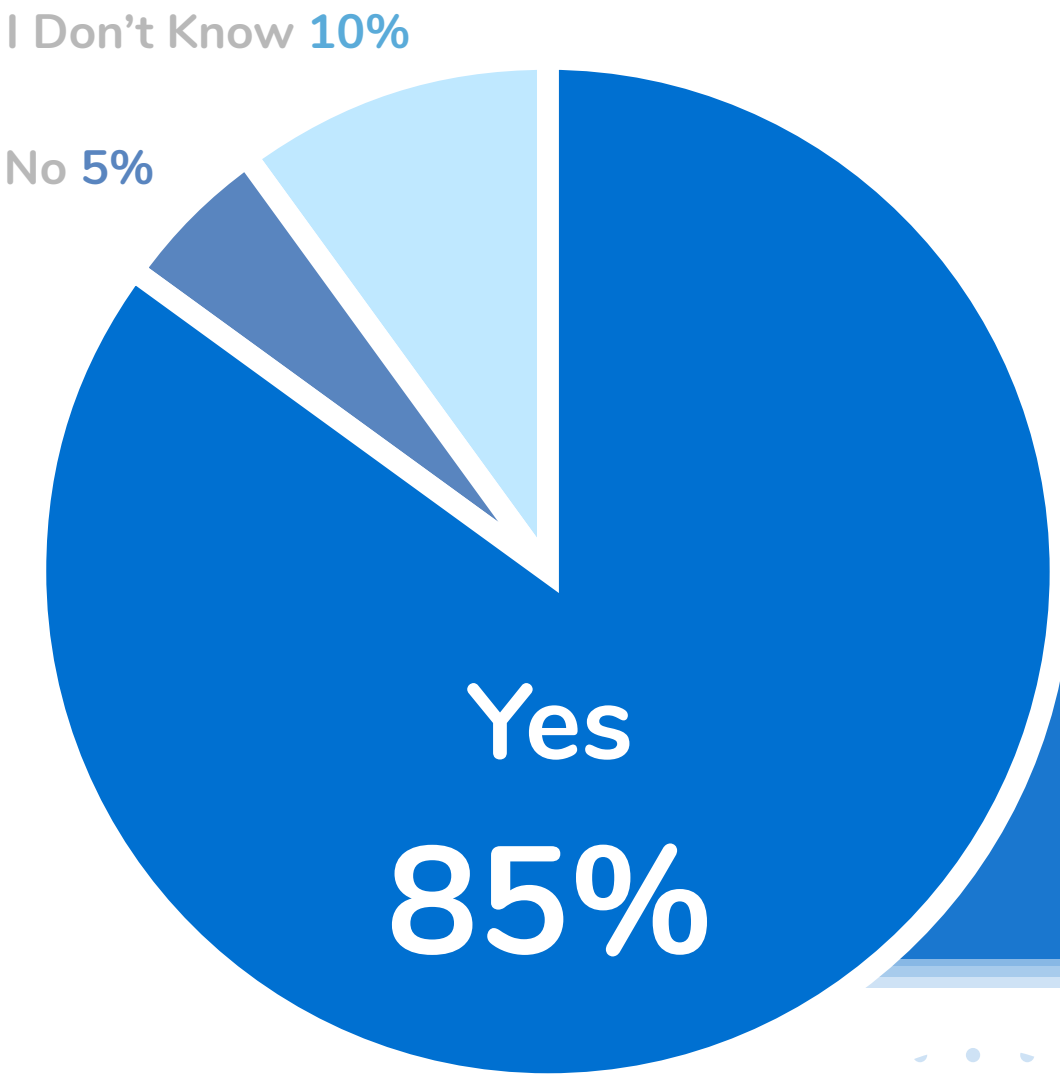
Awareness in Europe is higher across the board, with almost 66% having defined TOMS, and only 18% don't know, quite a contrast to the UK where over a quarter of organisations don't know if they've defined their TOMS.



C. Security policies and measures implemented in organisations:

Question 15

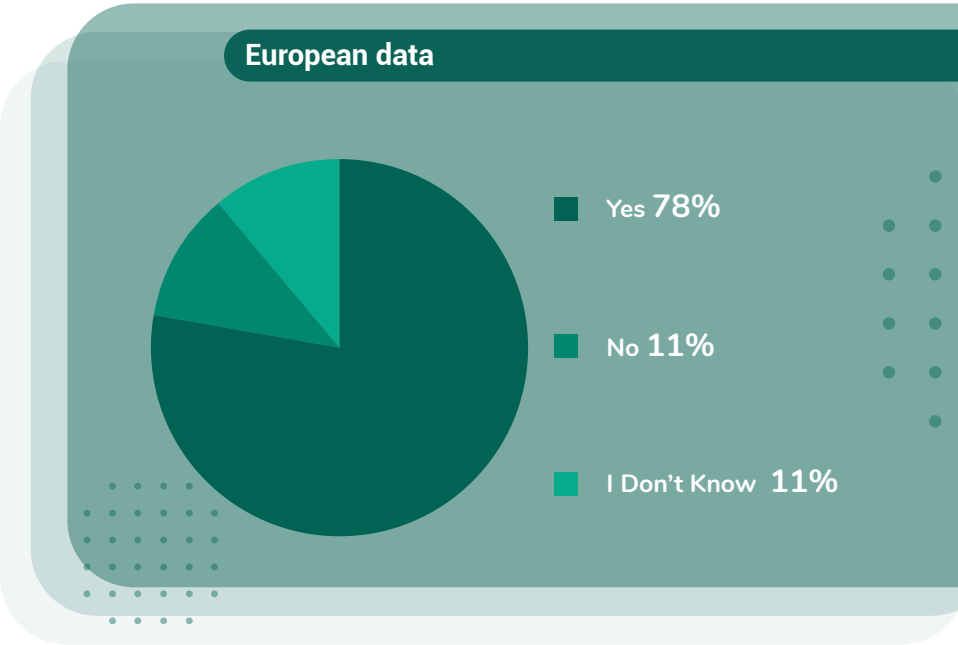
Does your organisation have a response protocol in place in case of a data breach?



A response protocol is a prerequisite, **the ICO is very clear in that any breach must be reported to the relevant supervisory authority within 72 hours,** and the clock starts ticking once you become aware of the breach. Part of a response plan includes robust breach detection and reporting procedures, this plays a big role in what we said earlier, damage mitigation, should a breach occur.

Contrary to the very high figures from the UK, only just under three-quarters of respondents on a European level have a response protocol in place, the UK does a much better job in terms of having a breach response plan.

In not having a response plan in place, valuable time is lost in the initial discovery phase. Instead of fast action that can mitigate the damage caused by unlawful access to data, time is spent figuring out who needs to do what.



Despite the effectiveness of data breach response plans, **the very fact that 15% of UK** organisations involved in the survey didn't have, or were unaware whether or not they have a response plan means it is extremely unlikely that they have one in place and are therefore **not compliant, more than two years after the GDPR legislation came into effect.**

04. Case study: how Yokeru has become GDPR compliant

Now we'll take a look at an example of what a successful data protection implementation should look like. We'll be using a client of ours, Yokeru, to see what was needed and how it was done, so let's dive in.

Yokeru is all about smarter healthcare, providing a way to better collect data in order to provide the best possible care for patients.

During the COVID-19 pandemic, medical care has suffered, there are no two ways about it. Many of the vulnerable in society who need medical attention simply haven't received it, those in care homes have been neglected two fold.

Firstly, when the government chose to prioritize the NHS over care homes when providing testing kits, **and secondly, because they simply couldn't get the care they needed, because much of the workforce that usually helps vulnerable people, was unable to get to them.**

This is where Yokeru proved itself to be so valuable. Automated phone calls that monitor the health and well-being of clients/patients enables the prioritisation of the most vulnerable in society.

Automation limits contact and vastly reduces time spent gathering information, allowing more time for actual treatment.

"Our technology monitors the health of the most vulnerable in our communities. As a result, we needed to be confident in our watertight GDPR compliance processes".

Hector Alexander | COO & Co-Founder at Yokeru

We've already looked into the critical importance of a data protection officer for data security and GDPR compliance and this is where Yokeru would face a problem. Not having a data protection officer meant that they weren't compliant with GDPR legislation at this time, and as they're treating highly sensitive data, compliance is a key issue for them.

We were able to help with this by providing our DPO service but also with another important aspect of compliance, the DPIA.

DPIA (Data Privacy Impact Assessment) is simply a preventative analysis measure to be undertaken before data treatment. Another critical activity that must be carried out, and yet there are many organisations that just don't do it, it's like driving without a license, sure you'll get away with it for a while, but eventually, you will get caught. Leading to potentially crippling fines and the long lasting knock on effects such as the devastation to reputation and loss of customers.

05. Conclusions

Recurring themes prevalent throughout the study are that **companies are generally aware of legislation and whilst they do attach importance to them, not nearly enough effort is made to ensure compliance.**

Failure to do so is in part due to lack of awareness of the penalties of non-compliance, it could be coupled with the thinking that many people are guilty of, 'it'll never happen to me', **what else could explain failure to comply with simple, inexpensive requirements** such as informing patients/clients about how their personal data is being treated.

Not being aware of legislation or severity of penalties results in many companies failing to achieve compliance, and these failings feed into each other.

But what do we mean by this?

Failing to have a DPO for example, is in violation of legislation, but also, an organisation without a DPO will find it more difficult to stay up to date with current legislation and be compliant with GDPR.

This is where failings feed into each other, non-compliance in this area, makes it difficult to succeed in others because as we said, having a data protection officer demonstrates compliance efforts, a DPO monitors compliance and provides vital guidance.

The success of Yokeru, in contrast to failings of Google with the Fit-Bit for example, (there was no opt-out choice for patients whose personal medical records were shared with Google under Project Nightingale) we see a clear competitive advantage that can be achieved through compliance with data protection laws (that's not to say Google and Yokeru are in competition here, it's just an example of good vs bad health data protection).

When vast amounts of resources are utilised looking to gain even the slightest competitive advantage in overcrowded markets, it's an easy win to give your company the edge that your team is always desperately looking for.

> **"The health care system is, as has been proven again, the lynchpin of our society.** *Digitization is also making the healthcare industry take a decisive leap forward, but it is also making it more vulnerable. The sector should take extensive security measures to prevent breaches of data protection laws".*

Lisa Hofmann | Chief of Legal Operations, Pridatect

"Given the global health situation, we would expect to see an increase in companies and technology solutions dealing directly with health data. *What is worrying is how they can manage this sensitive data. Each of these organisations must be 100% committed to data security. I believe that there is awareness in the health sector about compliance with GDPR but there is a lack of knowledge about the requirements they have to meet. It is clear from the results of this study that although a small percentage of the organisations recognize that they do not comply with GDPR, 22% do not have a DPO, and this is obligatory in any organisation that deals with this type of data on a large scale according to article 30 of GDPR".*

David Casellas | CEO de Pridatect

The observations from the experts is clear, healthcare is seen as increasingly important, and this special category data is at even higher risk, and steps must be taken in order to comply with legislation and more onus should be put on preventative measures to prevent the scrambling after a breach has occurred and mitigate any damage.

Pridatect simplifies the process of detecting risks and protecting data

DETECT AND IDENTIFY RISKS

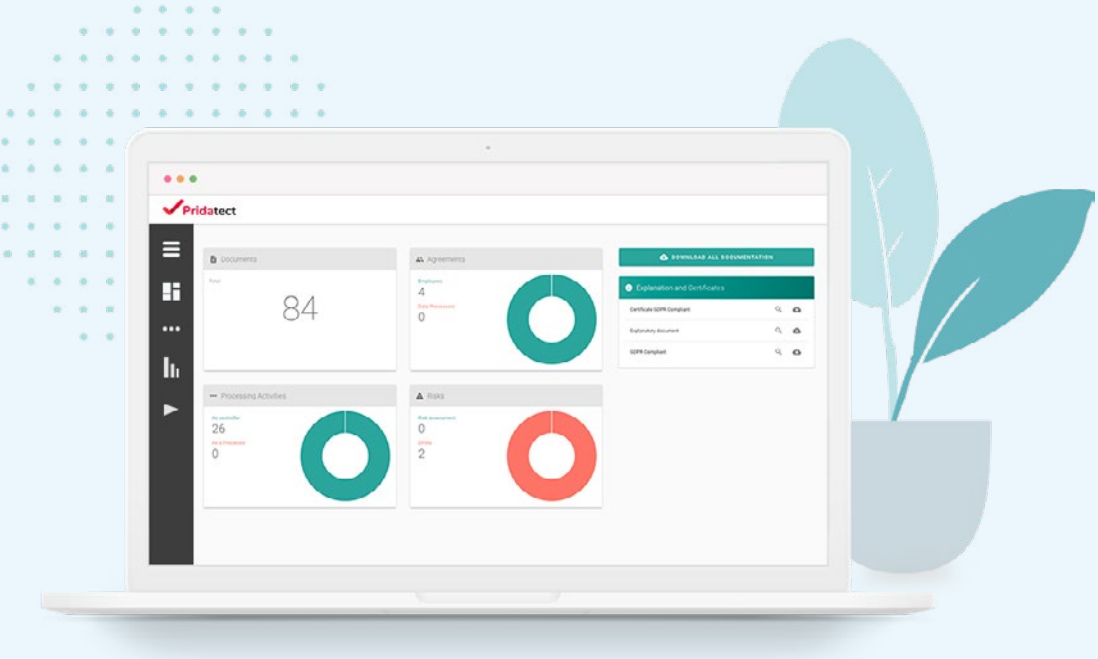
Detect and identify personal data treatment (customers, employees, suppliers ...) risks in your company. With the Pridatect platform we can identify and analyze threats and vulnerabilities in your data processes.

DEFINE AND SUGGEST PREVENTIVE ACTIONS

Knowing the risks in your company allows you to define the necessary measures to reduce and mitigate them. Pridatect helps you with the definition and suggestions of measures for your company.

MONITORING AND IMPLEMENTATION

Data protection is an ongoing task within a company. Pridatect does not only help with the initial implementation, but also with ongoing risk monitoring, measures, and the data protection related task management among your company's employees.



Contact us for a **free demo**
or make use of our 7 day **free trial!**