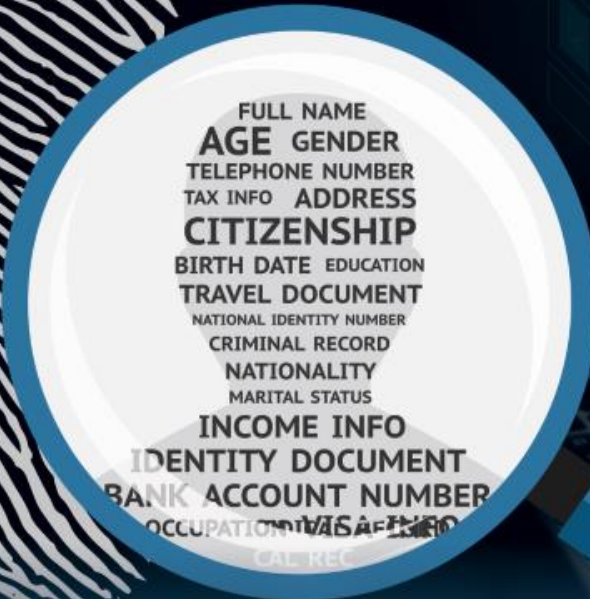




Management  
Consultants



# GDPR

General Data Protection Regulation

January 2018

# General Data Protection Regulation (GDPR)

The European Parliament has formally approved the EU's general data protection reform package, which includes General Data Protection Regulation (GDPR).

The final text of the GDPR was published in the EU Official Journal and the provisions will take effect on 25 May 2018.

Effective  
**May 25, 2018**



# GDPR Strict Restrictions



25th of May

2018

GDPR is coming...  
and you can't afford to ignore it!

Change is on the horizon. This time next year, things will be very different. The new [General Data Protection Regulation](#) (GDPR) will be fully enforced across Europe by May 2018.

Or else...



Penalties can amount to  
**20 million €** or **4%**  
of global revenue

# ICAP GDPR Survey



## Profile:

- Date of Research: December 2017
- Respondents: 210 Companies of all sizes and market sectors
- Response Rate: 4%
- Methodology: e-questionnaire



# Survey Results - Findings - Insights



# GDPR Awareness

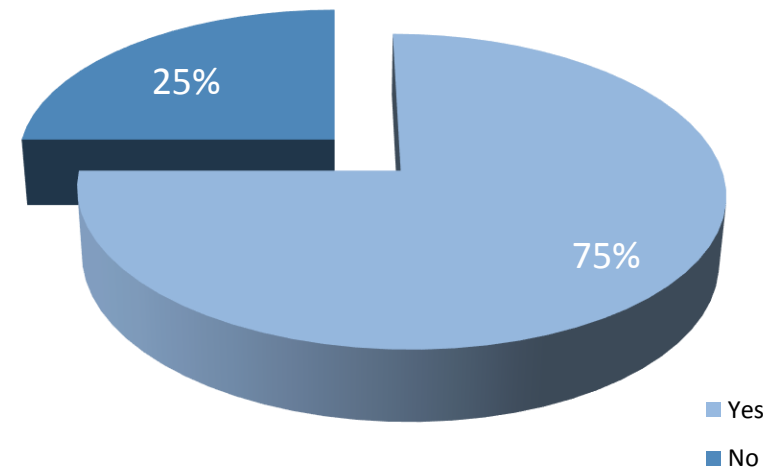


The General Data Protection Regulation (GDPR) has been approved by the European Union and once it comes into force in May 2018, will provide data subjects with significant new rights over how their personal data is collected, processed, and transferred by data controllers and processors. Does it demands significant data protection safeguards to be implemented by organizations?

So we asked the Market

**Do you know the New European Privacy Policy GDPR?**

The Outcome clearly indicates a high awareness of the new regulation

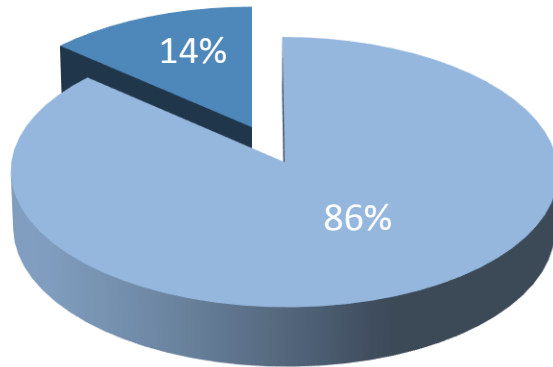


# GDPR Awareness by Company size (by number of employees)

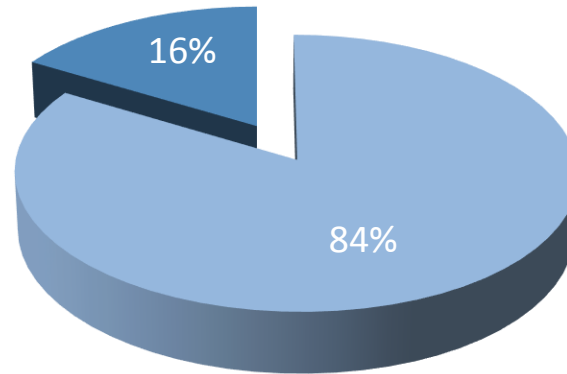


Are you aware of the New European Privacy Policy GDPR?

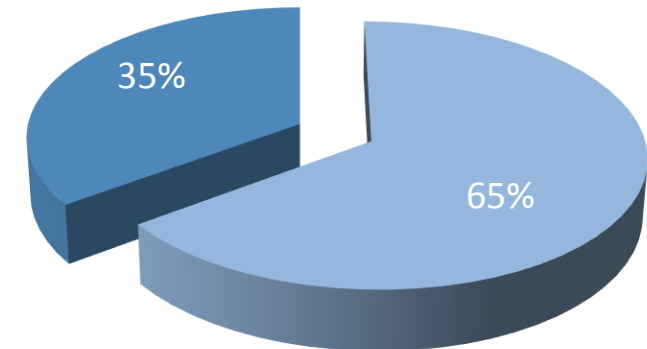
> 500



101 - 499



100 <



■ Yes  
■ No

# Definition of Personal Data

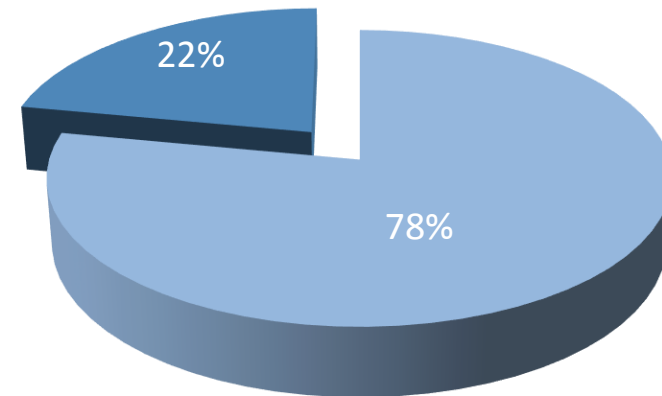


Personal data is "any information related to an identified or identifiable natural person". Direct identifiers include name, ID number, and online identifiers (e.g., email address), and indirect identifiers include location data and various types of identity. The personally identifiable information that will be relevant in the context of the GDPR includes data subjects' network identifiers, images, hobbies, political preferences, religious preferences, sexual orientation and other information about EU residents.

So we asked the Market

**Do you know the definition of Personal Data?**

Surprisingly the vast majority claims mass awareness and clear understanding of the definition of personal data



■ Yes  
■ No

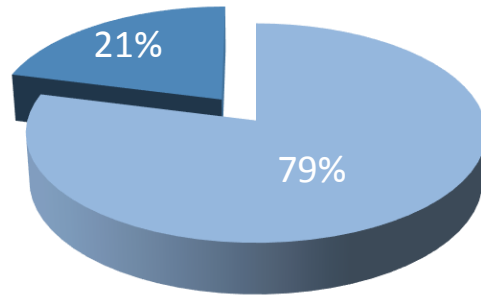


# Definition of Personal Data (by Sector)

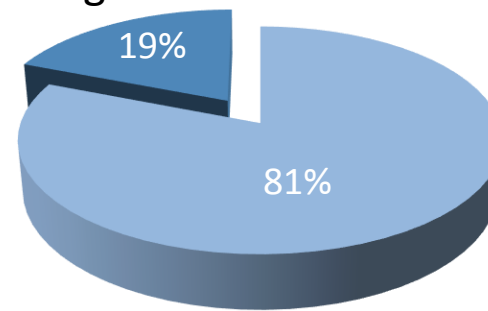


**Do you know the definition of Personal Data?**

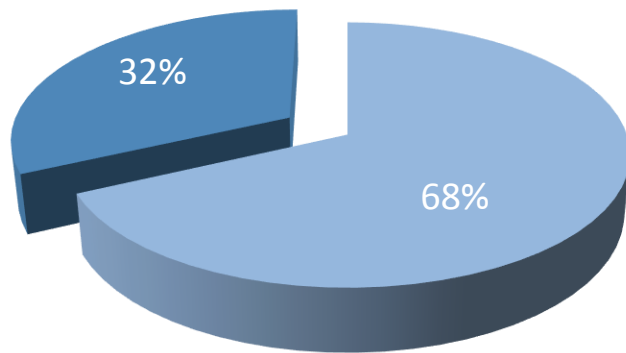
Trade



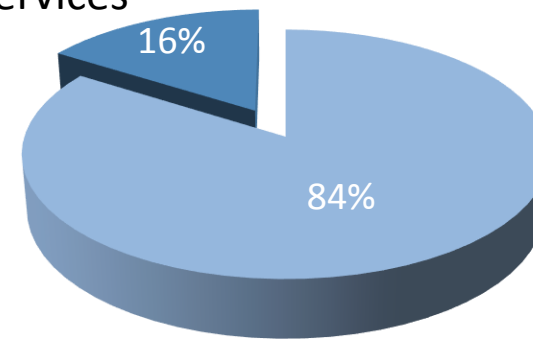
Manufacturing



Tourism



Other Services



■ Yes

■ No

# Personal Data Processing

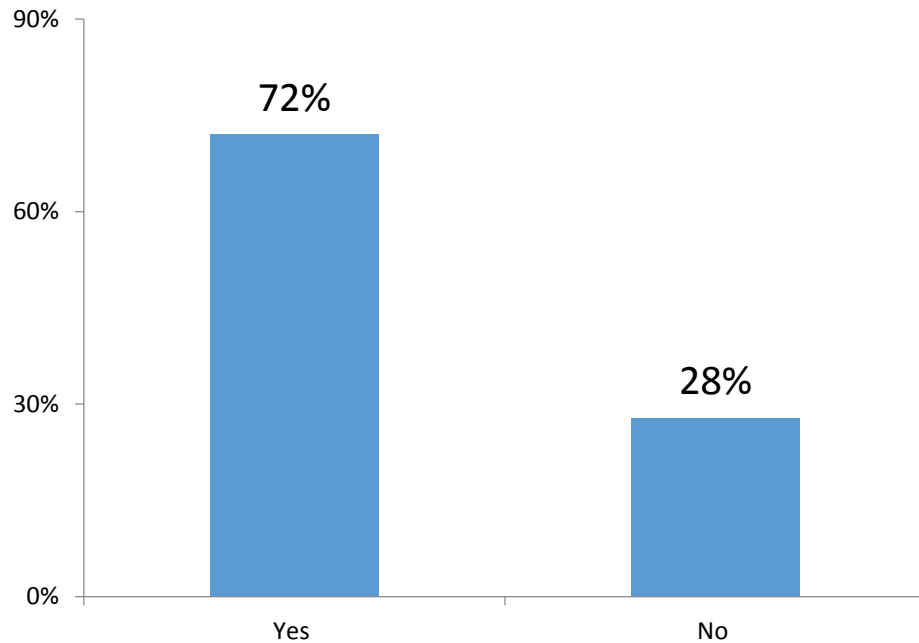


Demonstrating compliance with GDPR includes having policies on how to protect data under your control, an up-to-date assessment of risks to personal data (e.g., unauthorized or over privileged access), workable technical measures that enforce protection, rules on transferring data to other countries

So we asked the Market

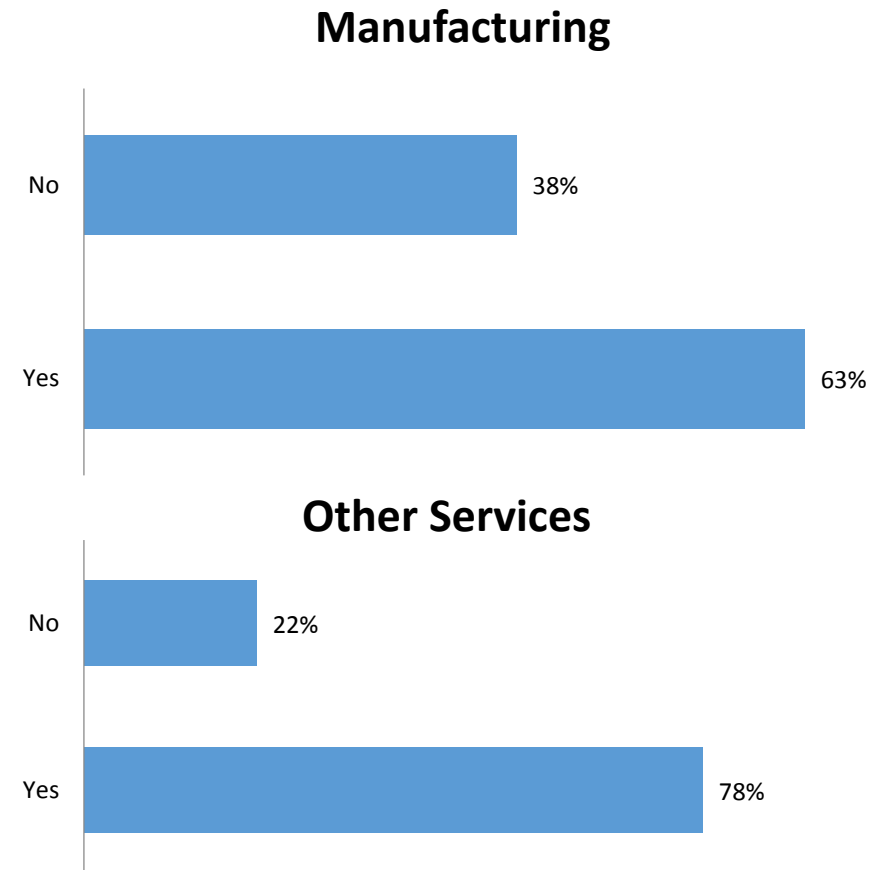
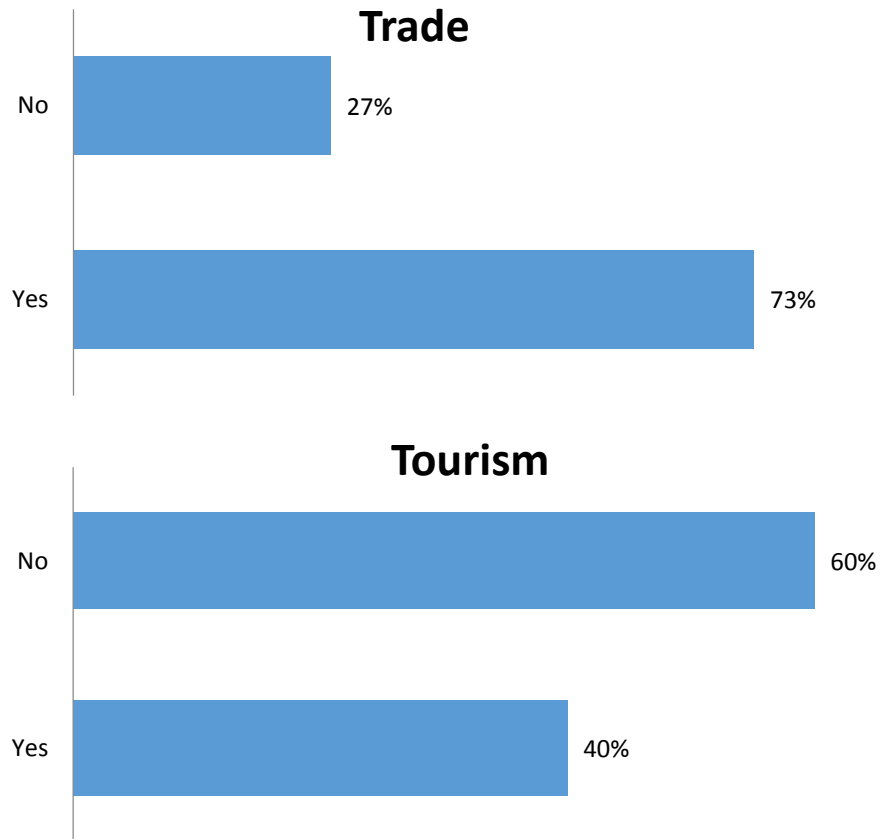
**Apart from employees, do you process personal data of your clients and / or partners?**

The majority of Companies replied by confirming their focus in analyzing customers as well as partner data



# Personal Data Processing (by Sector)

Do you process personal data of your clients and / or partners?



# GDPR Compliance

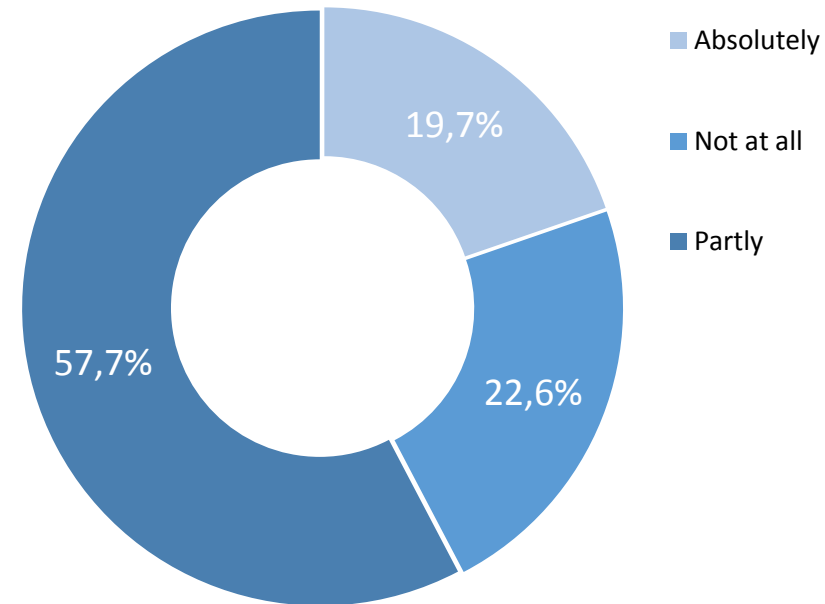


Complying with GDPR is not optional. If your organization controls or processes personal data on natural persons in the European Union, GDPR certainly applies to you. There is a whole host of requirements and mandates that need to be in place when GDPR comes into force.

So we asked the Market

**Do you know your level of compliance with the new GDPR ?**

The outcome clearly highlights the issue of compliance and the need for an action plan in view of the deadline of May 18

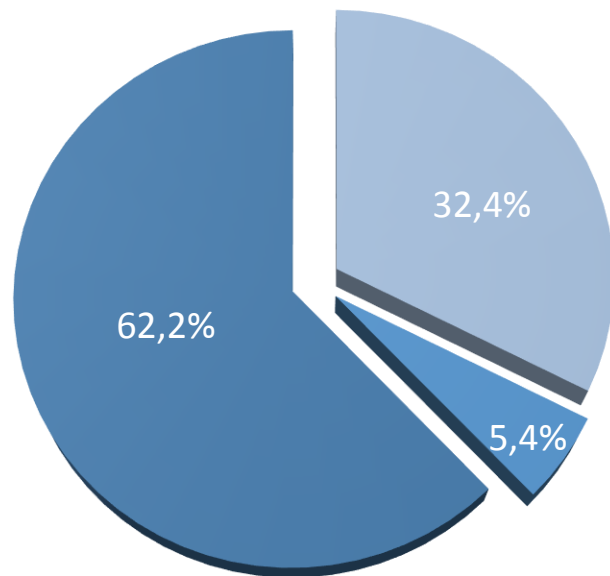


# GDPR Compliance by Company size (by number of employees)

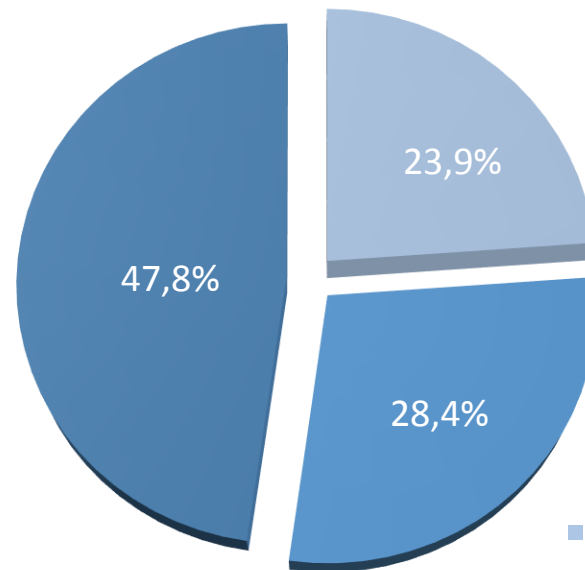
Do you know your level of compliance with the new GDPR ?



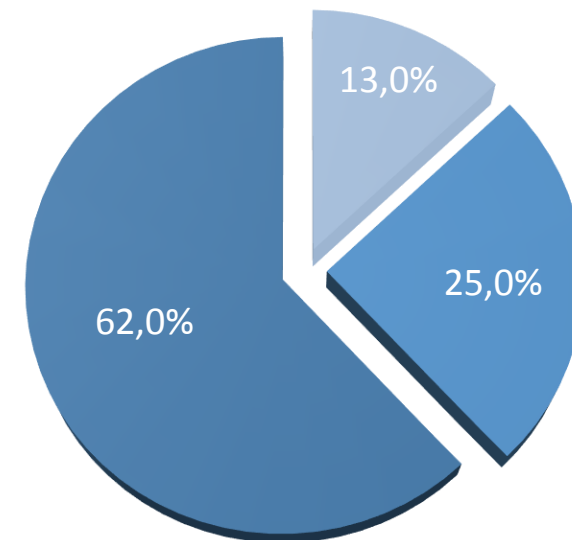
> 500



101 - 499



100 <



- Absolutely
- Not at all
- Partly

# Data Protection Officer DPO

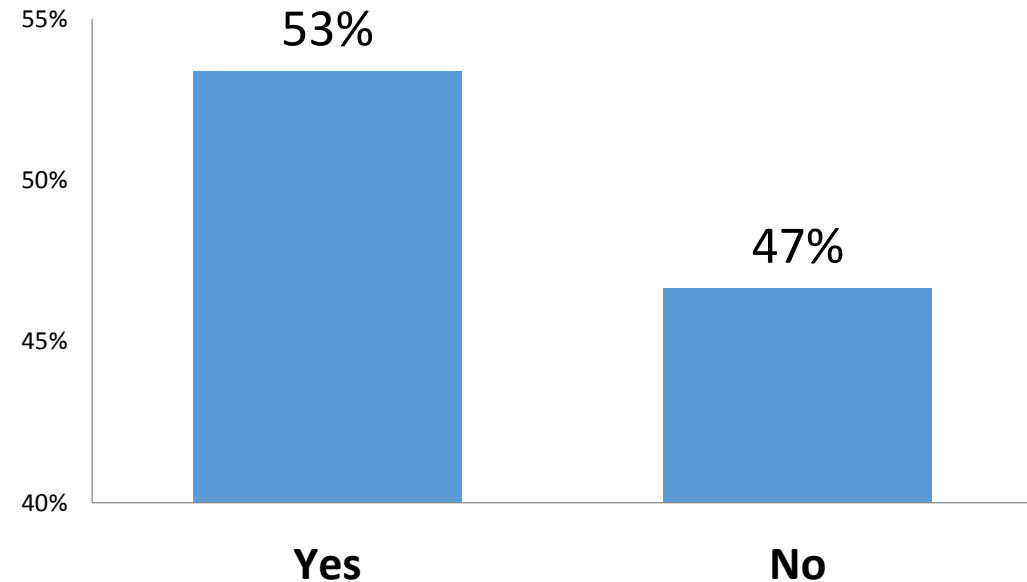


A Data Protection Officer (DPO) is an enterprise leadership role required under certain conditions by the General Data Protection Regulation. Data protection officer is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

So we asked the Market

**Do you know if your company will be required to appoint a DPO under the GDPR?**

The outcome shows that only half of the companies have a clear view on the issue.



# Training

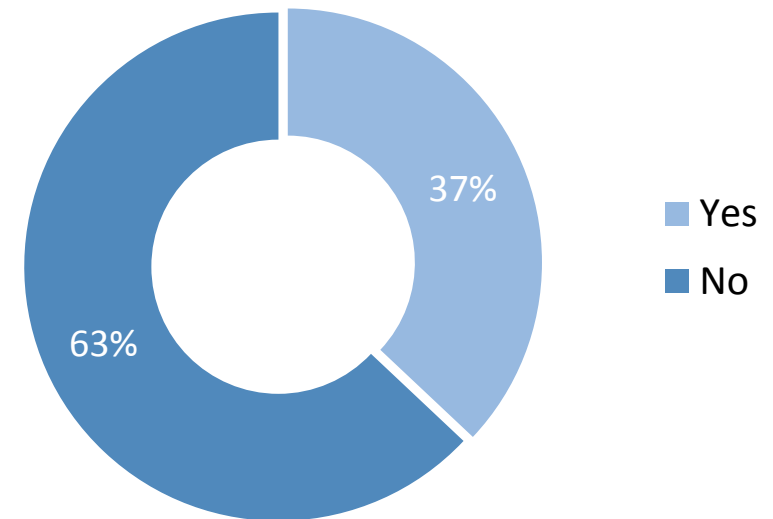


In view of new GDPR implementation, there is a definite need for training for anyone who processes personal data of EU citizens (employees, clients etc). GDPR future changes highlights the key issues that might affect you as a business and will help you determine the next steps for the training of your personnel.

So we asked the Market

**Have you trained your staff on security and privacy issues and practices?**

Census outcome shows that the majority of the companies has not started training their employees yet as per GDPR guidelines and restrictions



# Personal Data Collection

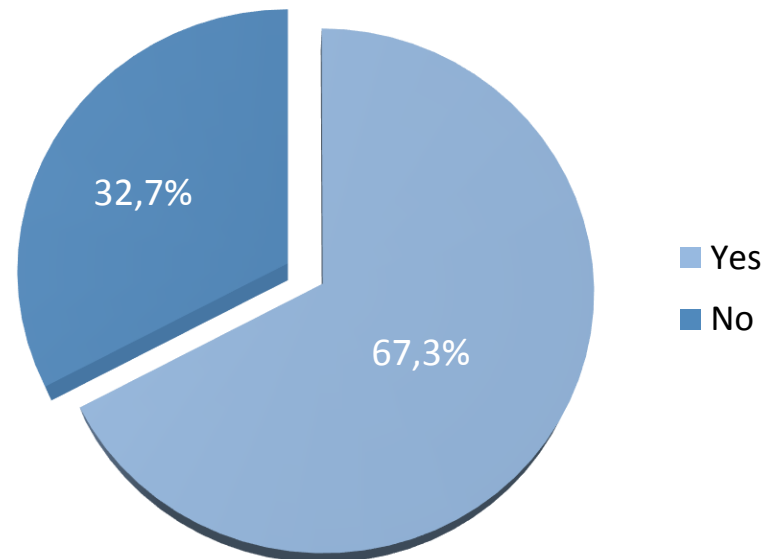


Organizations that control or process personal data must meet protection mandates, including gaining specific consent from data subjects, record keeping, notification of data breaches, and having the organizational and technical means to respond to the rights of data subjects in a timely manner

So we asked the Market

**Do you collect Personal Data on the basis of a trade agreement with the individuals - customers (purchase of product / service, subscription, etc.)?**

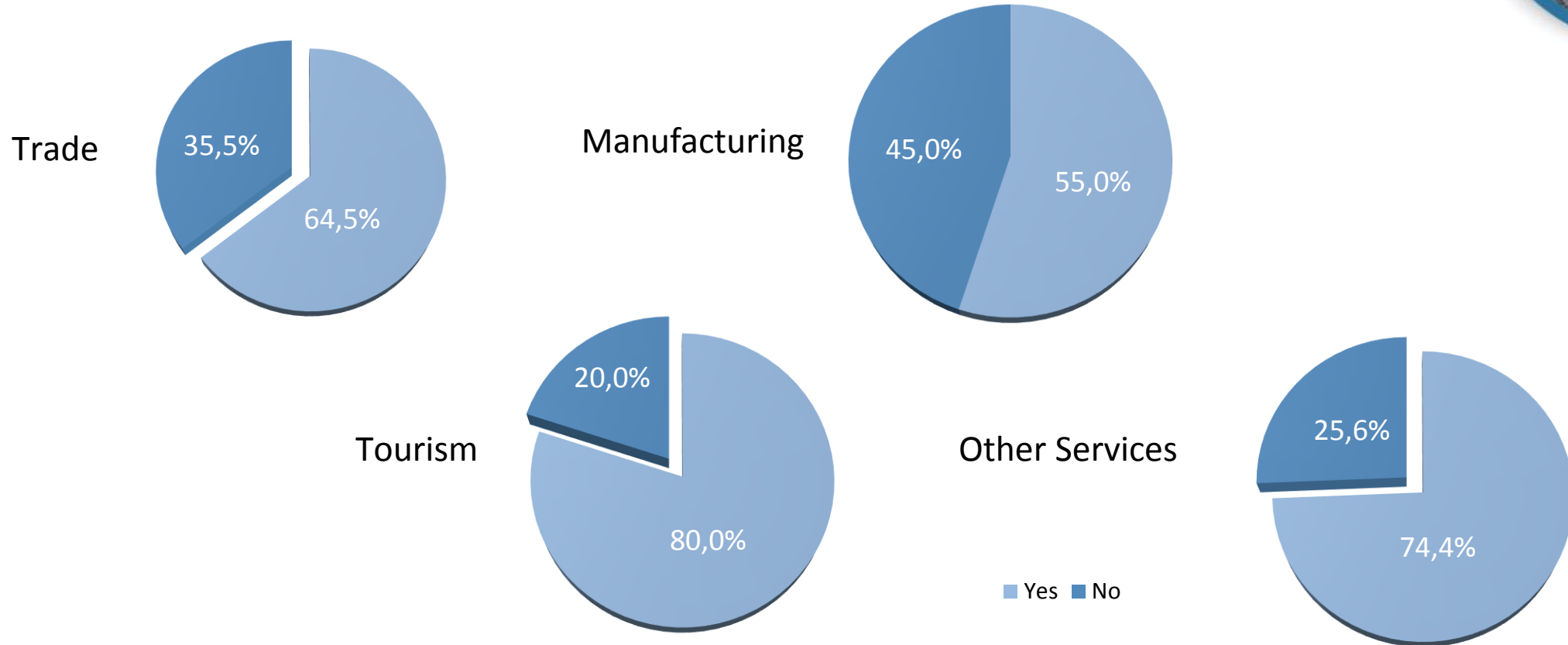
Census outcome indicates that the majority of companies in Greece formally exchange data with their customers / partners





# Personal Data Collection by Sector

Do you collect Personal Data?



# Data Transfer

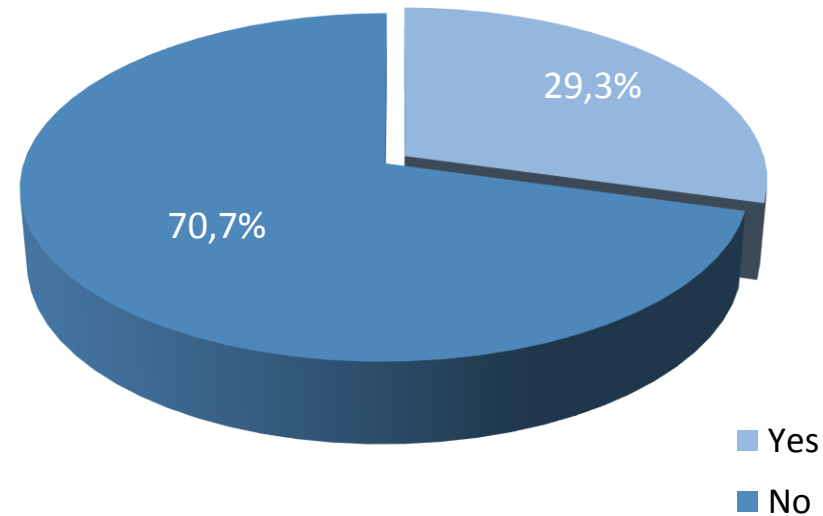


Prevent data from being transferred unless specific protections are in place. These protections can be an adequacy decision by the European Commission. The controller or processor has appropriate safeguards in place and legal remedies available, such as Binding Corporate Rules, among others.

So we asked the Market

**Do you transfer Personal Data you have collected to third parties?**

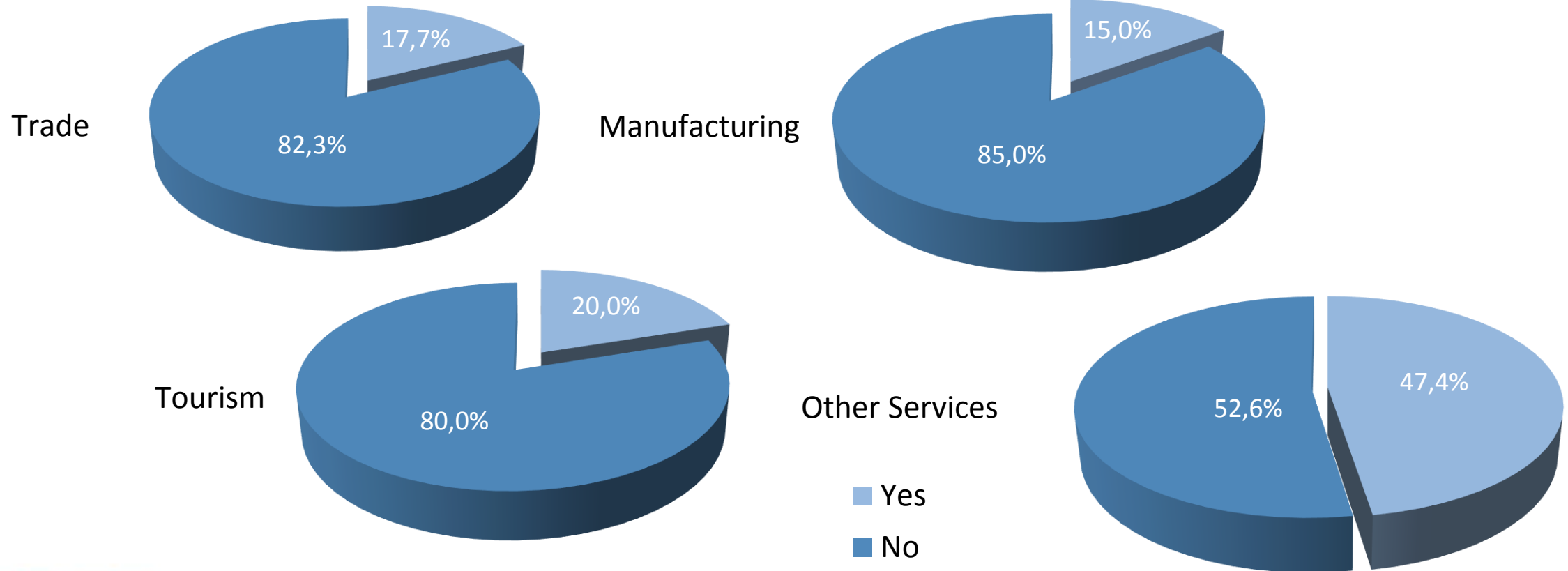
71% of the companies claim that they do not transfer Personal Data by any mean, a finger which is dramatically increased in Services Sector



# Data Transfer by Sector



Do you transfer Personal Data you have collected to third parties?



# Security Level

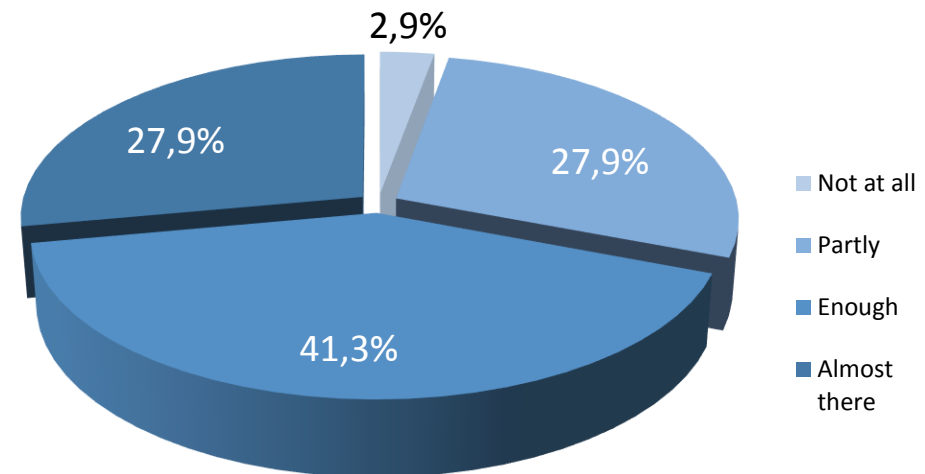


Ensure the protection of data during processing activities, through the implementation of "appropriate technical and organizational measures". These protection safeguards are to be implemented when determining how to carry out a processing. Technical and organizational security measures such as pseudonymization, encryption, processing system confidentiality, integrity and resilience, and a regular testing process for ensuring the security measures actually work.

So we asked the Market

**How confident are you about the level of security and protection of your systems and thus the personal data you process through them?**

It seems that the majority of the companies feel confident that they have a well protected security system in place

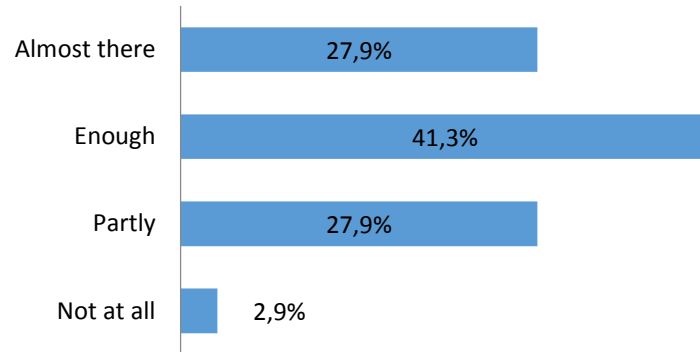


# Security Level

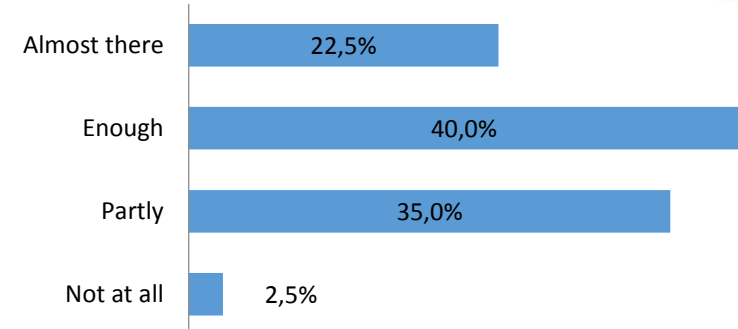
How confident are you about the level of your security?



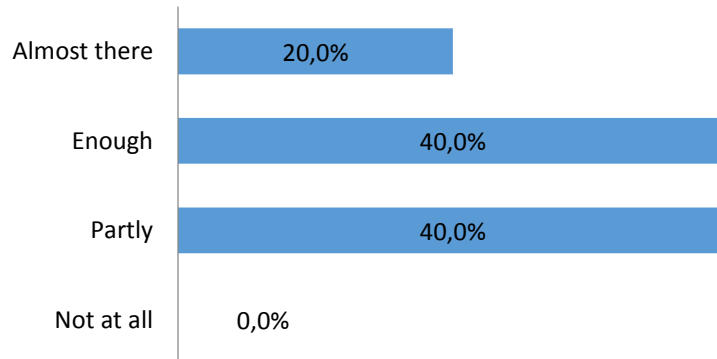
## Trade



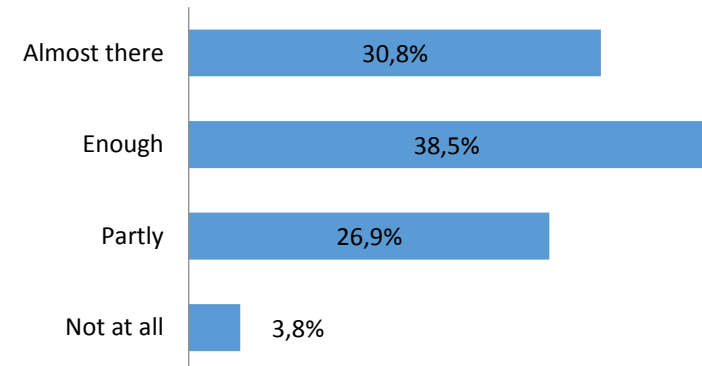
## Manufacturing



## Tourism



## Other Services



# Security incident

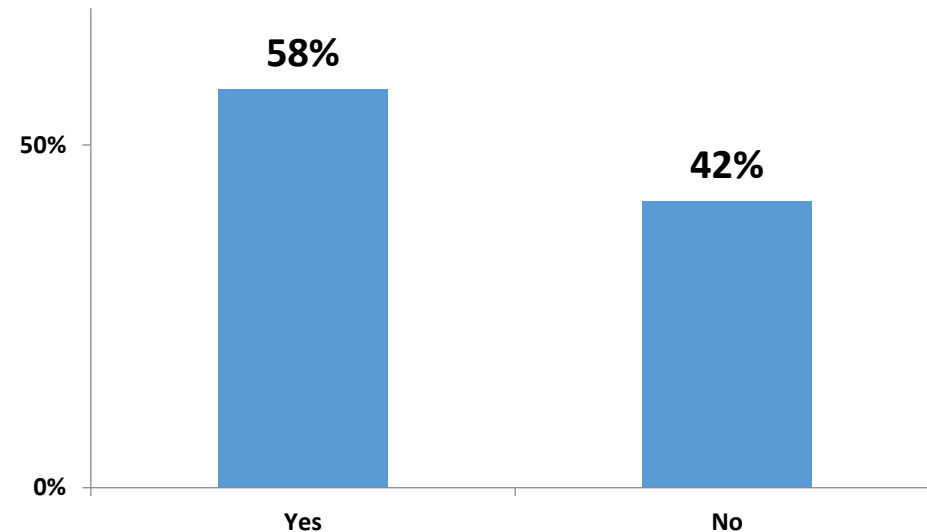


There are a whole host of requirements that need to be in place when GDPR comes into force, not least of which is that when a data breach occurs, the local data protection authority and all affected data subjects must be notified within 72 hours.

So we asked the Market

**Do you know what to do in case of a serious security incident and / or personal data leakage?**

Most of the companies replied positively to our question however our one-to-one meetings have shown that there is a gray area on the level of readiness in more complex incidences



# Personal Data and Individual Rights

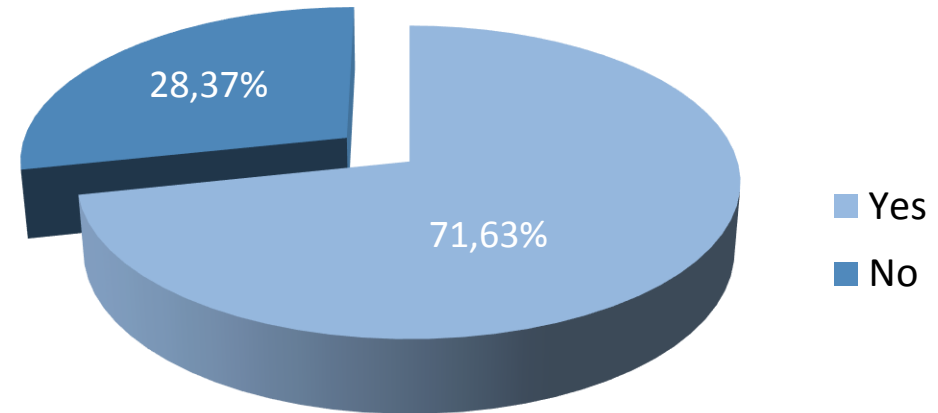


The General Data Protection Regulation (GDPR) once it comes into force in May 2018, will give data subjects significant new rights over how their personal data is collected and processed, by data controllers and processors. It demands significant data protection safeguards to be implemented by organizations.

So we asked the Market

**Do you know the rights of individuals whose personal data you process?**

Vast majority claims that they have a clear understanding and knowledge of the Individuals rights with regards to Sensitive Personal Data



# Consent of Subjects

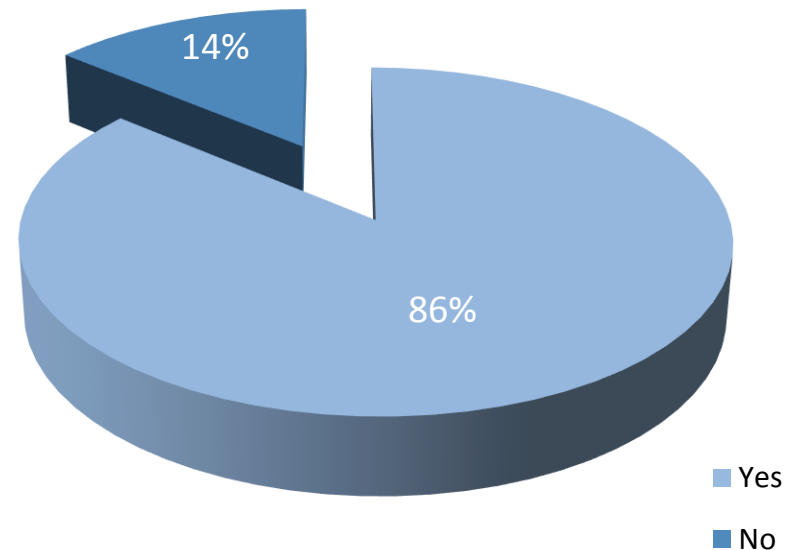


Consent is one among six legal basis for processing data. When required consent must be documented. Among other criteria, consent cannot be bundled, and the data subject must be able to withdraw consent just as easily as they gave it.

So we asked the Market

**Do you know if the consent of Subjects (individuals) for the collection and processing of their Personal Data is necessary?**

Vast majority claim positive awareness concerning the necessity of the consent by individuals





# DPO Assignment



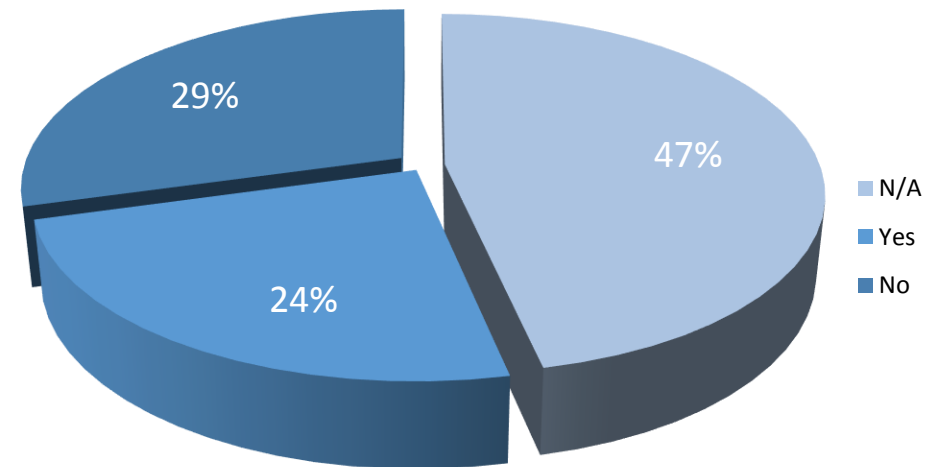
Under the new regulation, the data protection officer (DPO) must have "expert knowledge of data protection law and practices,". Such obligations include informing and advising the controller and processor of their obligations under GDPR, monitoring compliance, and being the liaison person with the supervisory authority.

The DPO must "directly report to the highest management level", and is to be afforded independence in carrying out his or her tasks.

So we asked the Market

## Have you assumed / assigned responsibilities for a Data Protection Officer (DPO)?

Small number of companies confirmed the assignment of a DPO while almost half of the companies reported lack of knowledge or ignorance

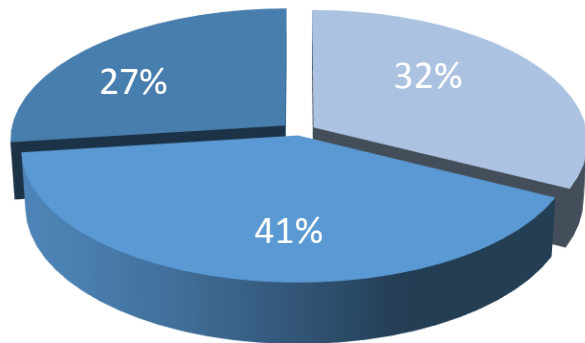


# DPO Assignment by Company size (by number of employees)

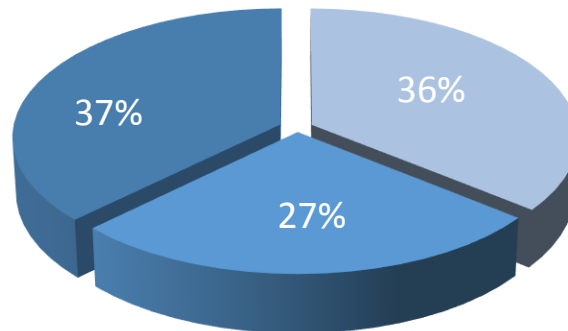


Have you assumed / assigned responsibilities for a Data Protection Officer (DPO)?

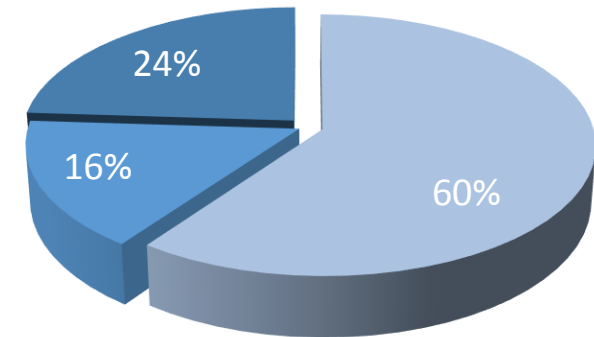
> 500



101 - 499



100 <



- N/A
- Yes
- No

## Key Notes

- ✓ 40% of SMEs lack awareness, of the new regulation
- ✓ uncertainty or lack, of compliance reaches 80% of SMEs
- ✓ Almost 50% of uncertainty recorded regarding DPO role and its necessity
- ✓ only 1 out of 3 companies have recognized the importance of privacy and security training
- ✓ Security controls framework has been positively recognized by the majority (70%) of the companies
- ✓ In contrast 42% of participated companies are not sure of their obligations during and after a data breach incident

## Survey Insights

- General Data Protection Regulation (GDPR) is here to stay!
- GDPR remains a grey area for Greek businesses
- Companies state of readiness and understanding have great potential for development / adaptation
- SMEs exhibit the lowest degree of General Data Protection Regulation awareness

## Outcome

Considering that the GDPR was only formally announced recently, it appears that there is a good level of understanding amongst the companies which responded to the questionnaire.

Although, there is a realization that a lot of work is needed to become compliant, the majority of the survey participants show significant percentage of uncertainty regarding their readiness status or compliance plans. Similarly, a gray picture is noted regarding the DPO role and its necessity, as well as the data breach notification obligations.

It is worth to note that the uncertainty percentage is higher for the SMEs who need additional information and guidance towards GDPR compliance.



FULL NAME  
**AGE GENDER**  
TELEPHONE NUMBER  
TAX INFO ADDRESS  
**CITIZENSHIP**  
BIRTH DATE EDUCATION  
TRAVEL DOCUMENT  
NATIONAL IDENTITY NUMBER  
CRIMINAL RECORD  
NATIONALITY  
MARITAL STATUS  
**INCOME INFO**  
IDENTITY DOCUMENT  
BANK ACCOUNT NUMBER  
OCCUPATION VISA INFO  
MEDICAL RECORD

Για περισσότερες πληροφορίες Τηλ.: 210 7200117, e-mail: [MChamilothis@icap.gr](mailto:MChamilothis@icap.gr)  
e-mail: [consulting@icap.gr](mailto:consulting@icap.gr), [www.icap.gr](http://www.icap.gr), [www.icapconsultants.com](http://www.icapconsultants.com)