Grant Thornton

DPO Survey 2024: Cyprus Insights, and the role of the DPO

European survey 2024

Summary

01 Introduction

The function of the DPO within enterprises

Since the enforcement of the General Data Protection Regulation (GDPR) in May 2018, European Union member states, have been dealing with the implications and requirements of this landmark legislation. The GDPR is an improved reconstruction of data protection directives and laws from the past, for member states to keeping up pace with the rapid technological developments and globalisation that have been changing the way in which personal data are collected, accessed, and used. In Cyprus, as in other EU member states, Data Protection Officers (DPOs) play a crucial role in overseeing GDPR compliance within organizations.

During the closing of 2023 Grant Thornton Cyprus, in association with 10 Grant Thornton member firms in Europe launched a survey aimed at establishing an overview of the DPO function in the main European countries.

From our survey we obtained insights about the thoughts and considerations of DPOs in relation to their operational function and contribution within their organizations, and where we currently stand domestically in terms of compliance with the GDPR.

Christos Makedonas

Partner, Digital Risk

Grant Thornton Cyprus

Stavros Demetriou

Manager, Digital Risk

Grant Thornton Cyprus

02 Survey Sample Presentation

A representative population

Survey Sample Presentation

Within November 2023, in collaboration with 10 other EU based Grant Thornton member firms, we launched a survey aiming the input of DPOs in various sectors of the GDPR such as in Governance, Compliance Management and Security.


Cyprus


Spain


Italy


Ireland


Denmark


Slovakia


Netherlands


Czech Republic


France


Malta


Luxembourg

Majority of the companies responding to the survey were **SMEs**
<200 employees - **45%**,
200 - 500 employees **15%**
1.000+ employees **25%**

Almost **95%** of the DPOs work in the private sector and **5%** in the public sector

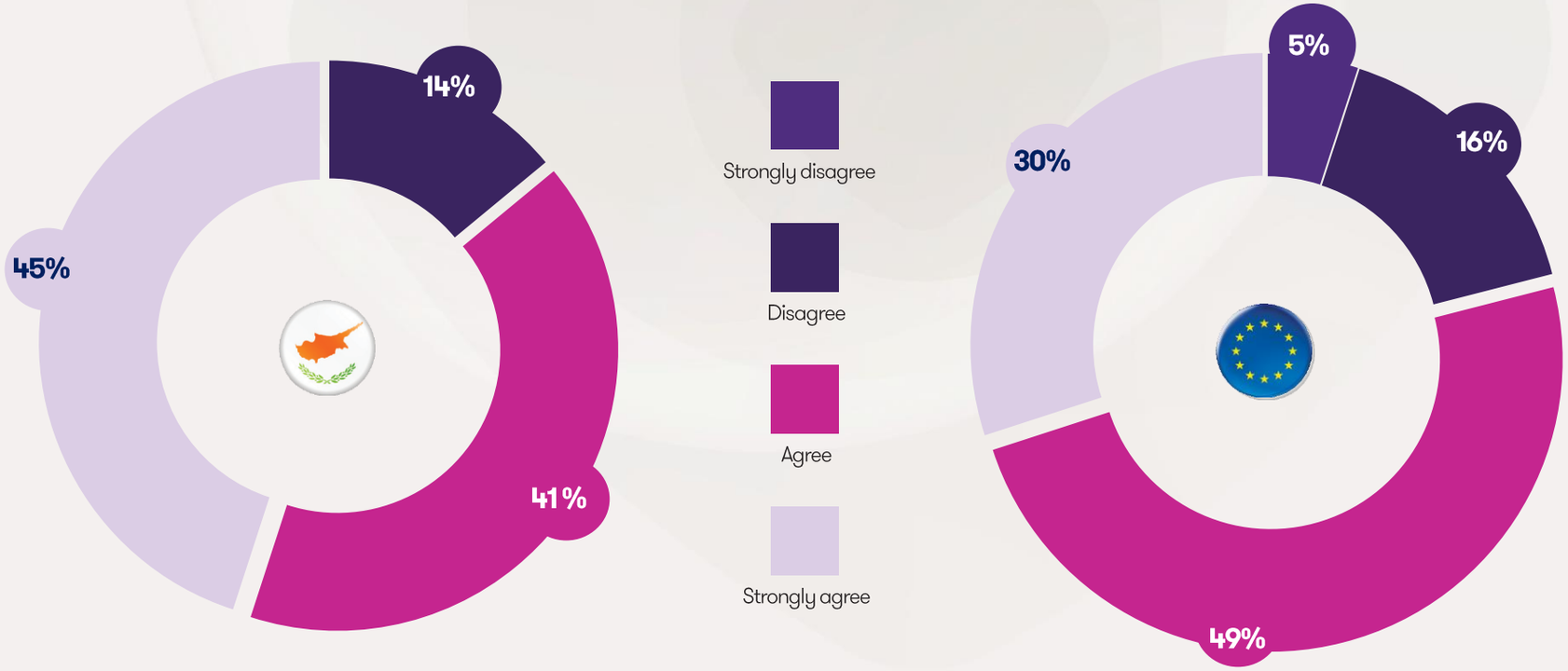
Main sectors represented:
Business Services (29%)
Banking & insurance (19%)
Manufacturing (10%)

03 Governance

Governance relating to GDPR - compliance not fully established in companies yet

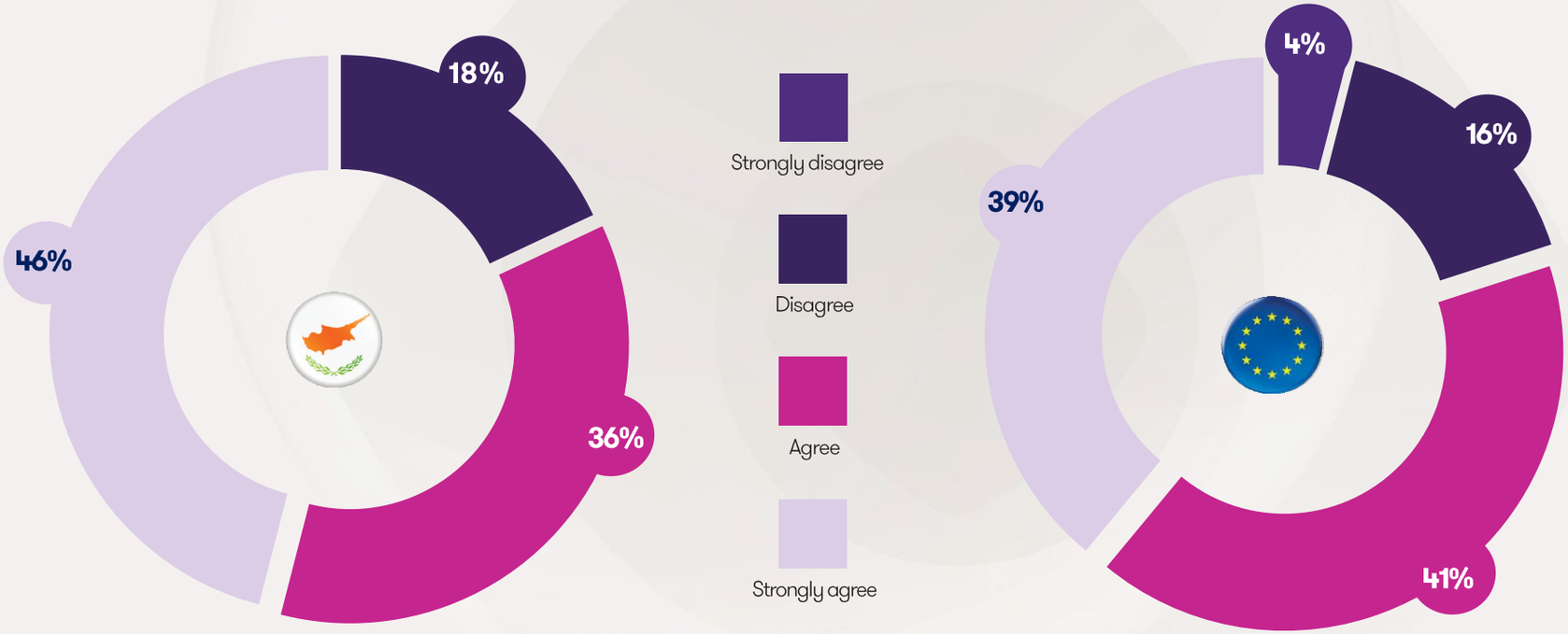
45% of the responders in Cyprus and 30% in Europe believe that the governance of the GDPR compliance is mature enough within their organization. While 14% of the Cypriot responders, and 21% of the European responders, believe that governance is not mature. Even 6 years after the enforcement of the GDPR, this subject remains relevant.

«The governance of the GDPR compliance is mature in my organization»



A hierarchical connection that satisfies the DPO

"The hierarchical attachment of the DPO in my organization is relevant"

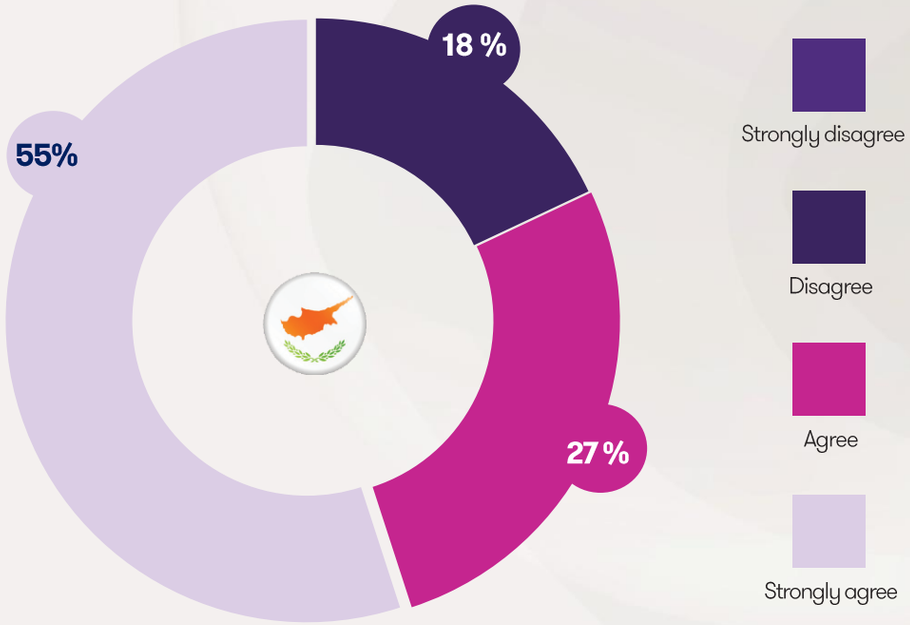


It seems that the hierarchical reporting of DPOs is generally perceived as satisfactory by them, since within EU as well as within Cyprus, only 20% and 18% of the responders respectively disagree with this statement.

In Cyprus, 82% of responders and 80% in EU believe that their hierarchical reporting is completely relevant.

Attentive Executive Management to data protection issues

"Executive Management is accessible and responsive to data protection issues"



82% of the responders in total in Cyprus, consider that their executive management is attentive to issues relating to data protection.

A small proportion of the responders expressed that their executive management is not attentive on data protection issues as they should had.

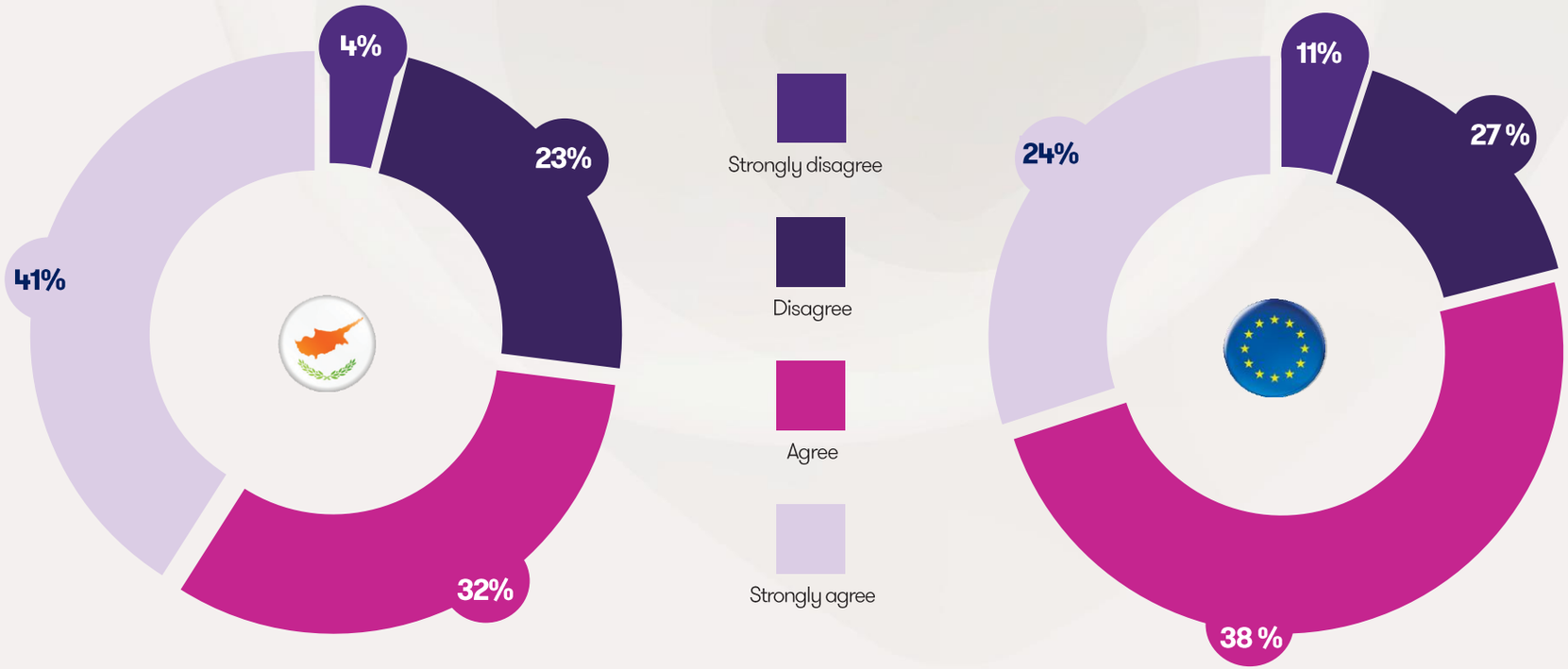
Resources provided are proportionate to data protection challenges

A high percentage of DPOs in Cyprus are satisfied with the resources invested by their organizations to maintain compliance with GDPR.

A total percentage of 73% of the local DPOs believe that the means allocated are sufficient to carry out their mission compared to the 62% of EU.

These results are not influenced by the sizes of the organizations since the responses are occurred to be homogeneous irrespective the size of the organizations.

"The means (employees and budget) allocated to the DPO are sufficient to carry out its mission"



DPO function

The DPO function finds its place mainly within 3 departments in most organizations.

- Internal Audit, Risk
- Legal
- General Management

Legal or Risk departments, can be argued that they can handle matters of GDPR as DPOs.

However, to achieve independence and ensure GDPR compliance, the DPO must be dedicated either as a separate department, or to operate within an existing department, however not holding other positions and/or responsibilities.

Company executives and general management are not suggested to hold DPO roles, according to the European Data Protection Board (EDPB) and Supervisory Authorities (SA).

The management must ensure that every responsibility of the organization under the GDPR is adequately handled.

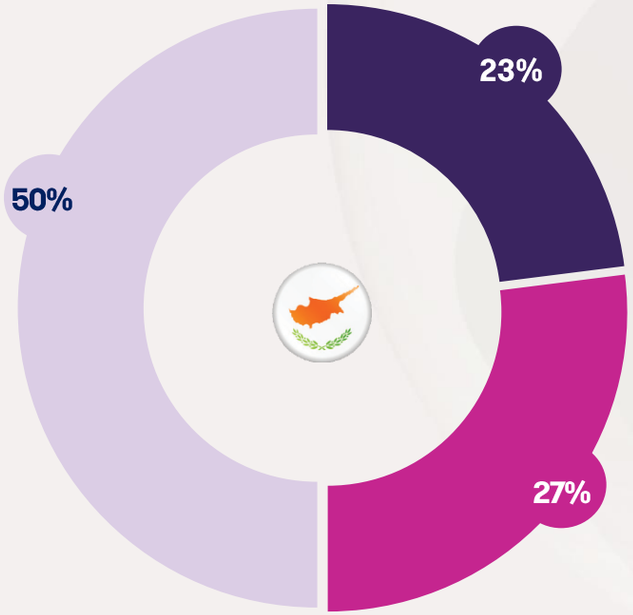
Under the GDPR, the DPO must be chosen based on his/her expert knowledge and qualities of data protection law.

A dedicated DPO with the appropriate expertise on the matter will focus exclusively on data protection and the overall support to the organization for compliance.

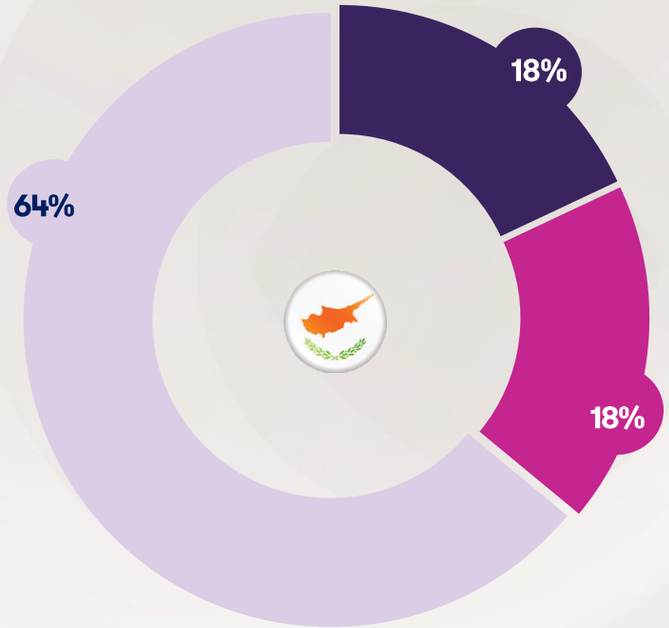
04 Compliance management

Compliance is steadily achieved

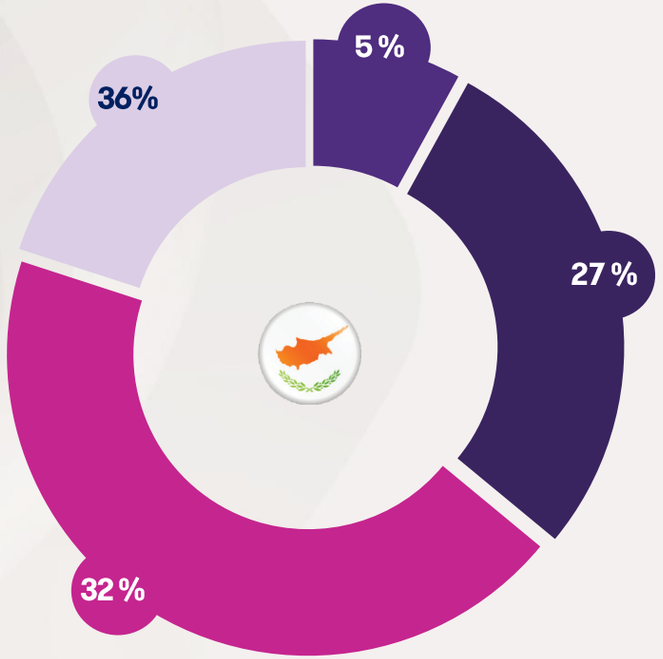
"The management of data subject right requests works well"



"Our contractual clauses are up to date"



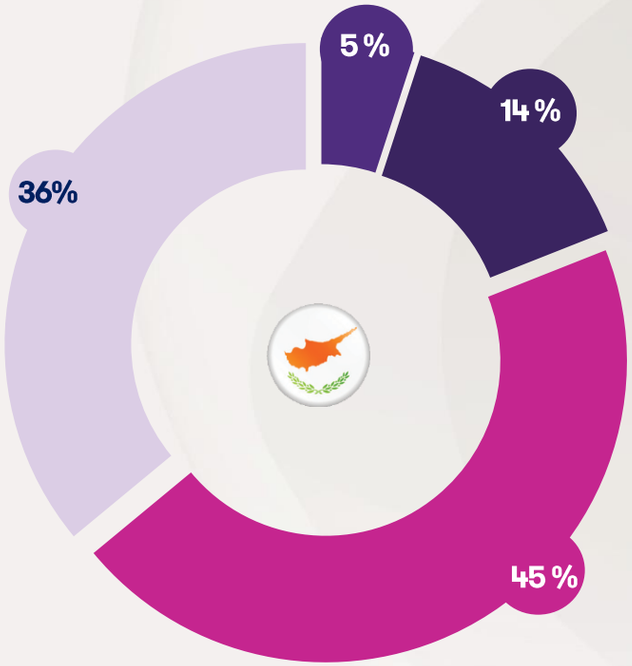
"I am satisfied with my data processing register"



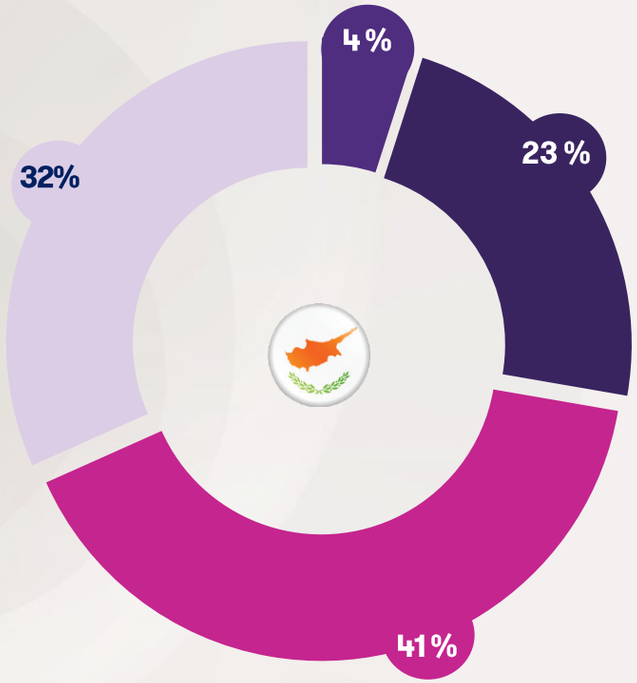
Strongly disagree | Disagree | Agree | Strongly agree

Compliance is steadily achieved

"My procedures are up to date or sufficiently known and deployed"



"I can assure that the principle of privacy by design is respected and implemented by operational staff"



A combined emphatic percentage of 81% indicates the confidence of the DPOs that the internal organizational procedures in relation to data protection are up to date and sufficiently deployed.

Similarly, 73% of the DPOs in total also are assured that the principle of privacy by design is respected and implemented by the operational staff.

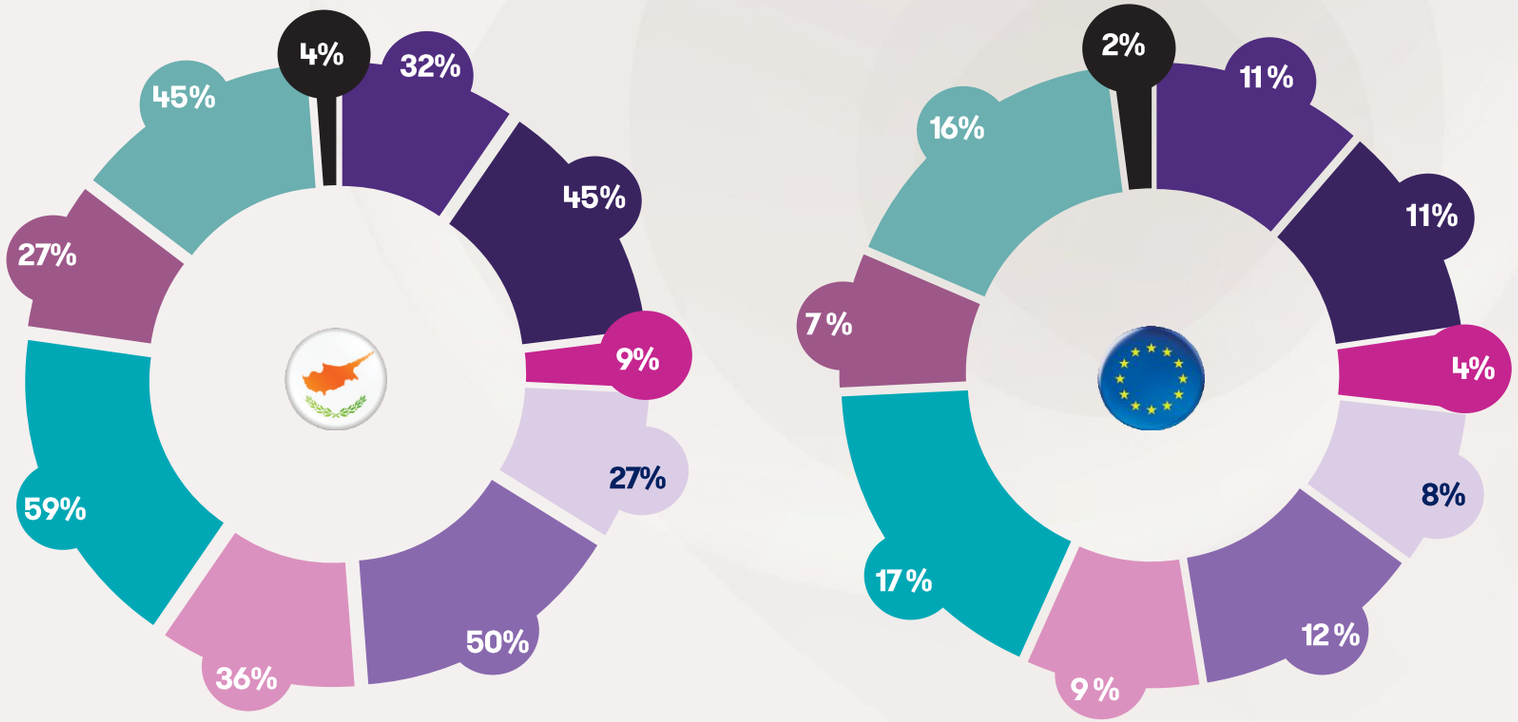
The above, results are quite encouraging, however it is reminded that data protection is a dynamic environment which requires consistent commitment to address emerging risks.

Main concerns of the DPOs

In Cyprus, similar with other European countries, the 4 main concerns of the DPOs are:

- Employee awareness
- Data transfers outside the European Union
- Privacy by design
- Data deletion

"What are your main current concerns?"



- Management of third-party compliance pledges, particularly questionnaires.
- Privacy by design.
- Cookies.
- Management of data subject right requests.
- Data transfers outside the European Union.
- Multi-regulation management at group level.
- Employee awareness.
- Employee data protection.
- Data purging.
- Other

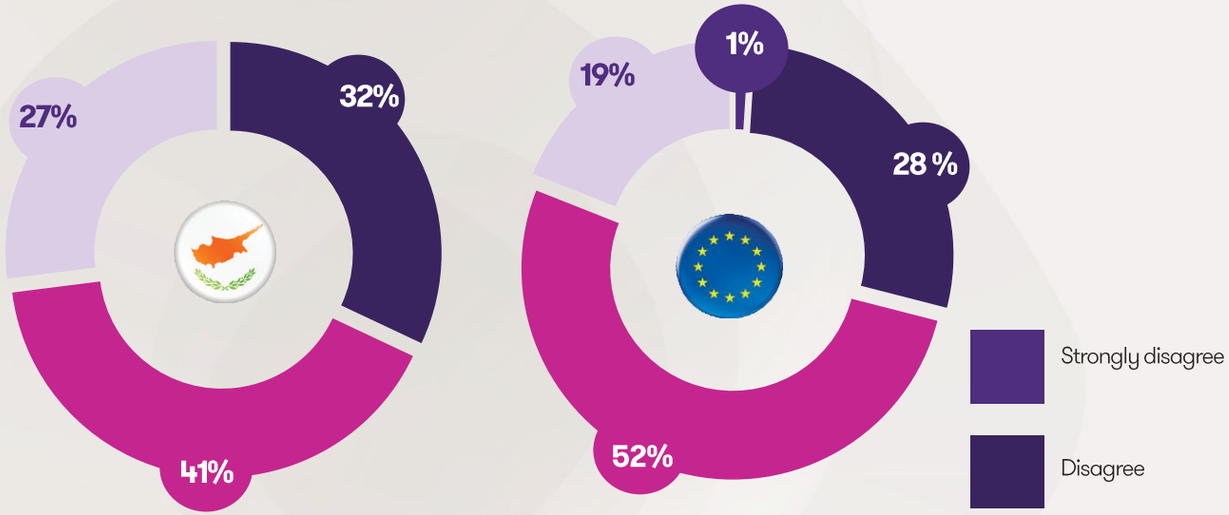
Raising employee awareness: an ongoing effort

The main purpose of raising awareness is not only to train employees on the GDPR, but to ensure they are aware of how their operational activities may impact the protection of personal data.

68% of the companies in total believe that their employees are well aware of the challenges of the GDPR in their daily tasks however 32% of them consider awareness levels insufficient.

Similar feedback was obtained from the European perspective since 71% of the companies in total believe the same.

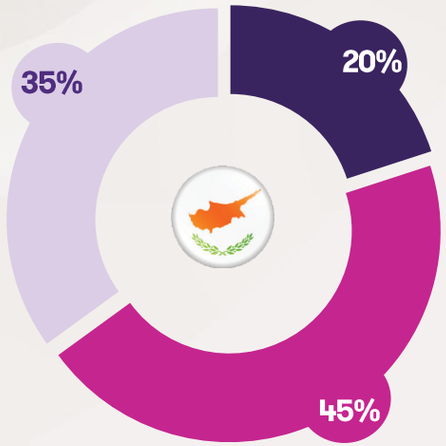
"Employees, in their daily activities, are aware of the data protection stakes"



In relation to awareness of data security (mainly IT) the results seem even better. This is in particular due to the collaboration of CISOs with the other departments within companies where they promote data security best practices. A combined percentage of 80% of the total companies expressed that employees are aware of data security issues.

The size of the companies has no impact on these results.

"Employees are made aware of data security issues"



DPO comments

> General training via e-learning is important however not sufficient. We need to be closer to the reality of the professions. E-learning should be combined with awareness training sessions each built and adapted to the several business industries.

> Training sessions are not only about the technical controls that should be in place. Staff awareness in relation to data protection should be embedded in the corporate culture.

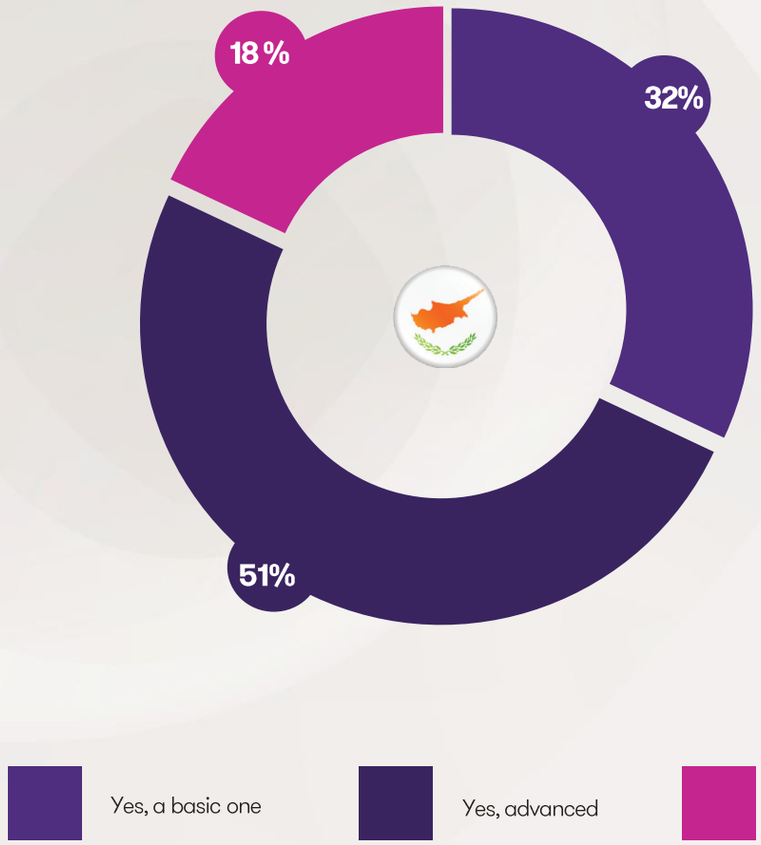
Equipping your compliance management irrespective the size of the company

Based on our survey, it was found that half of the companies (51%) utilise an advanced tool to manage their compliance with the GDPR.

A significant rate of 32% utilises a basic tool such as Microsoft Excel whereas an 18% does not utilise any kind of tool at all.

Digitalisation of the governing procedures in relation to GDPR compliance, enables companies to sufficiently monitor their level of compliance and provides a centralized action plan for all compliance issues.

"Do you have a GDPR compliance management tool?"



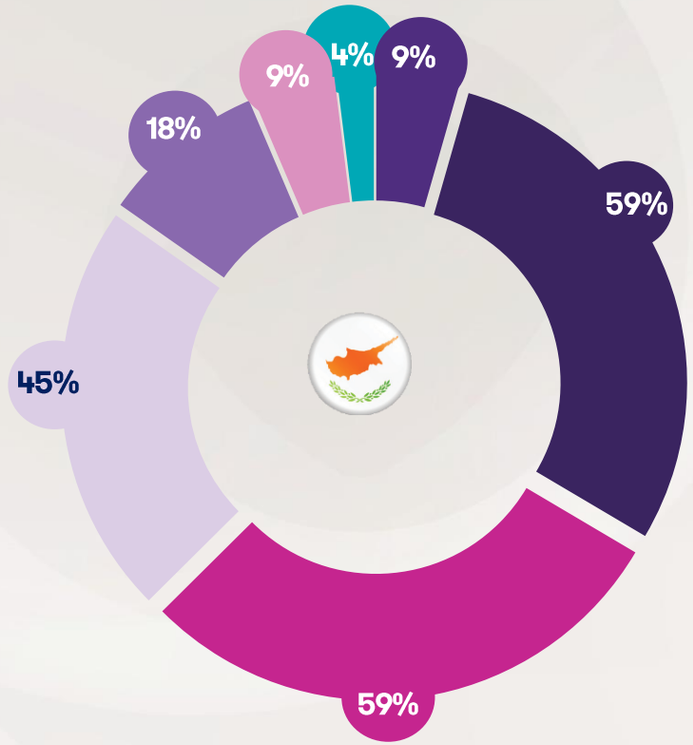
GDPR compliance monitoring system

The compliance monitoring systems are mainly distinguished in 3 groups:

- ✓ Audits executed by external service providers (i.e. consulting firms)
- ✓ Audits executed by the DPO of the company
- ✓ Internal audits carried out by internal staff

Similar results were identified within Europe as well, since compliance monitoring is mainly achieved through these 3 options.

"What compliance monitoring system have you set up?" (multiple options enabled)



- Compliance indicators reported by the GDPR correspondent.
- Audit by an external service provider.
- Audit by the DPO.
- Internal audit.
- Second-level controls integrated into internal controls.
- GDPR certifications (Europrivacy, GDPR CARPA).
- I do not carry out any control.

6 years elapsed

After 6 years, it is clear that operational compliance remains a hot topic.

Although most of the companies are addressing the main topics of the GDPR such as the management and execution of data subject requests, and the development of technical and organizational measures for the safeguard of personal data, many areas still need to be improved.

After six years of the enforcement of GDPR, it appears that processing records still need to be made more reliable, procedures need to be better deployed, and the subject of privacy by design to be systematically considered.

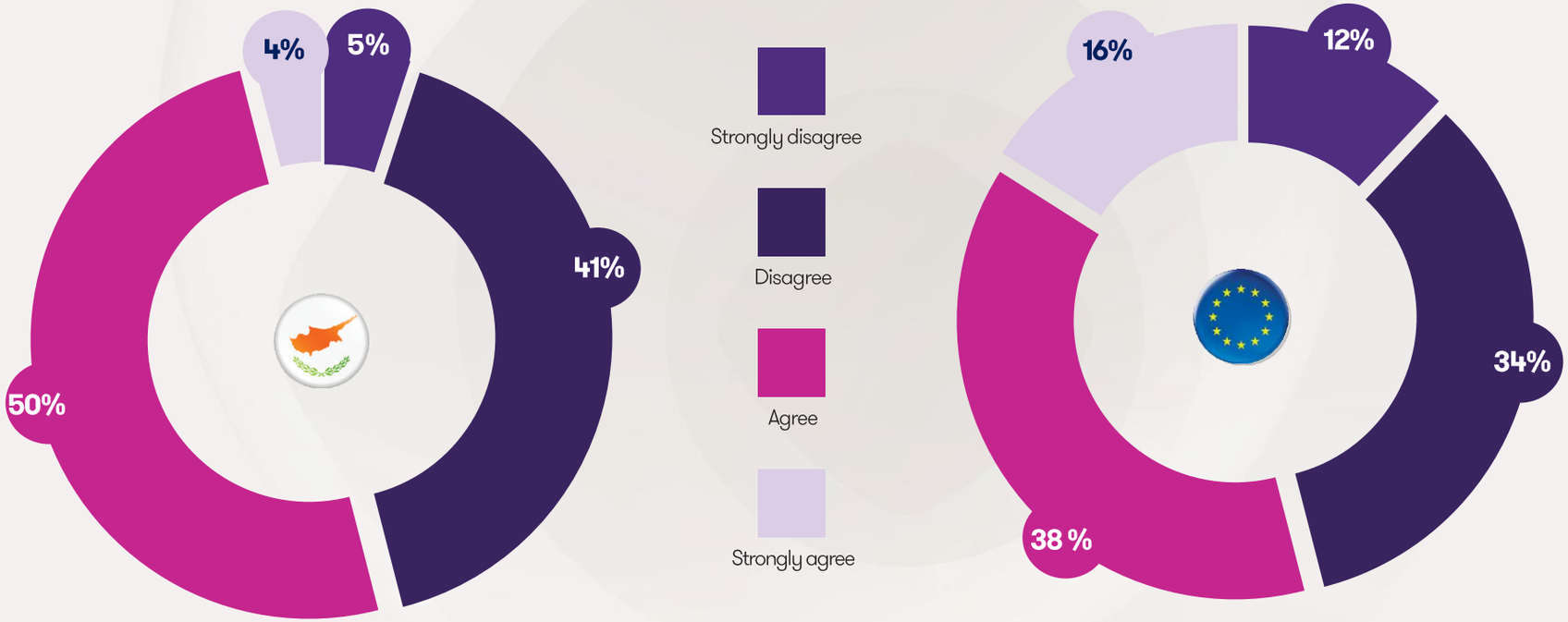
The main areas that should be improved highlighted by the survey are:

- ✓ Raising more operational awareness among employees is a necessary step and an essential lever for improvement. The DPOs are well aware of the importance of this area.
- ✓ The digitalization of compliance. The rate of equipped companies with a compliance management software (even if it has improved over the last years) remains insufficient. This lack of digitalization impairs on the ability of DPOs to follow action plans, and manage their network,
- ✓ and organizational compliance.
- ✓ Also, additional effort is required in order to maintain and apply in practice the defined retention periods in relation to personal data stored on corporate systems.

05 Data Security

Privacy impact assessments complication

“Privacy impact assessments are still difficult to carry out”



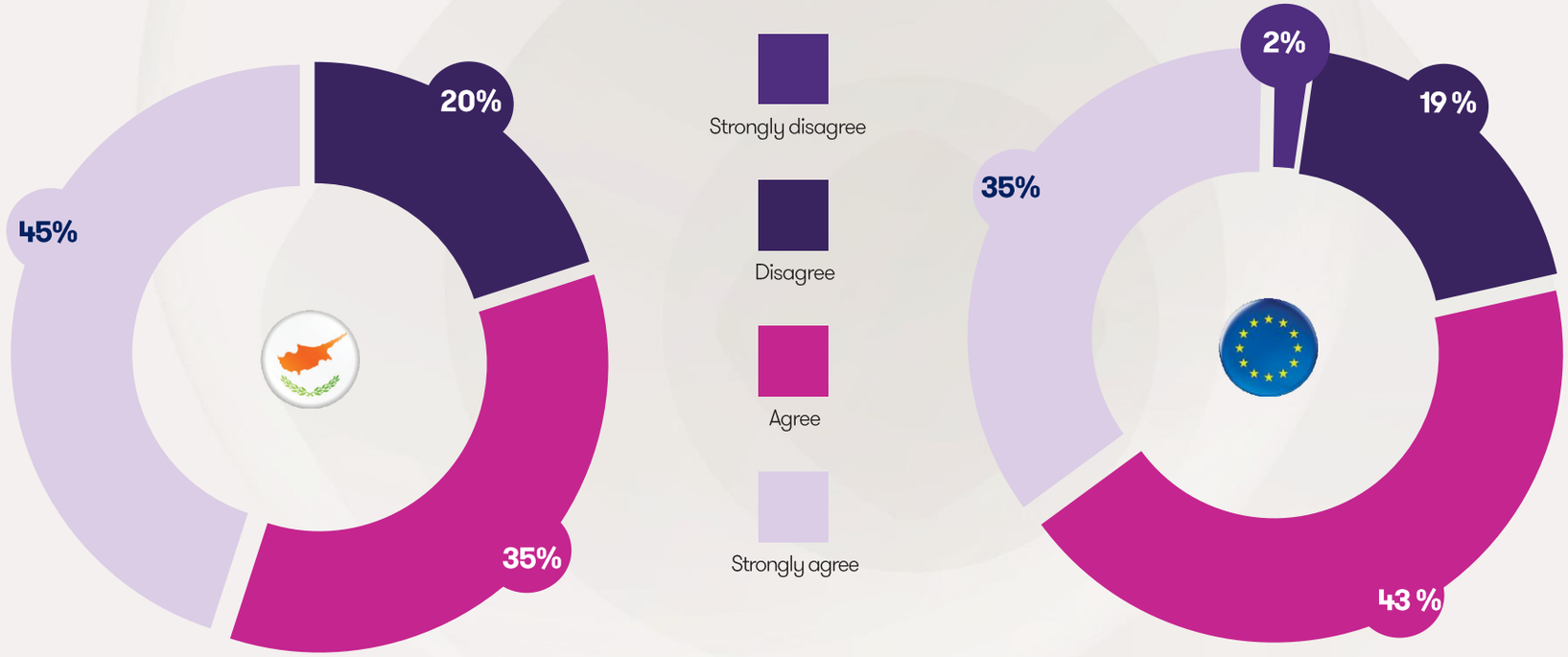
Half of the DPOs in Cyprus (54% combined) believe the privacy impact assessments are difficult to be carried out, same is believed on a European level.

This can be explained in particular by the following factors:

- The difficulty sometimes, to identify the need of carrying out a PIA, despite the guidelines provided by the Supervisory Authorities.
- The technical and complex aspect of the analysis that has to be carried out , which sometimes requires legal and technical expertise.
- The time which is required to perform the assessment as well as the effort of the subsequent monitoring.

A strategic partnership with the CISO

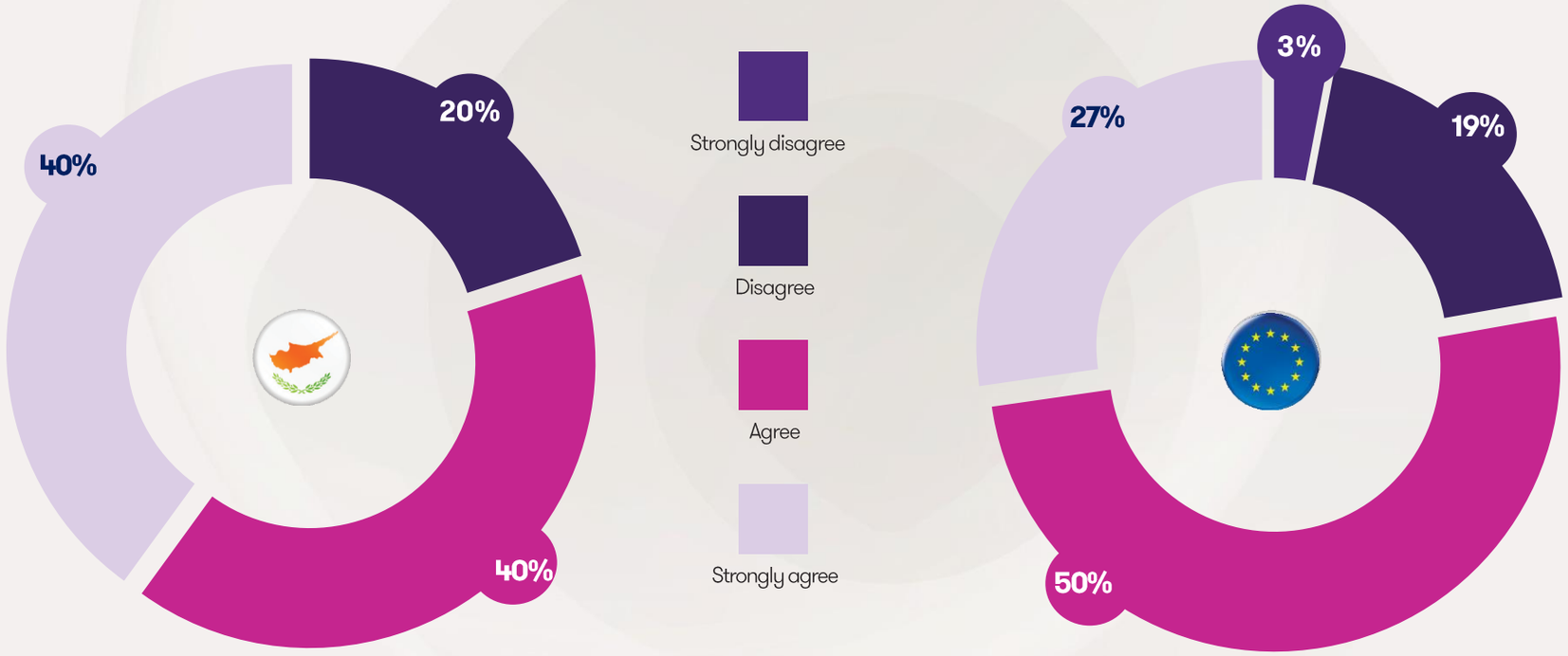
“DPO and CISO work well together”



The CISO is the preferred partner of the DPO, and the results of the survey are very satisfactory on the collaboration between these two functions. Indeed, in Cyprus as in Europe, nearly 80% of responders are satisfied with the collaboration with their CISO.

Data security principle

“Security measures are defined for each data processing operation”

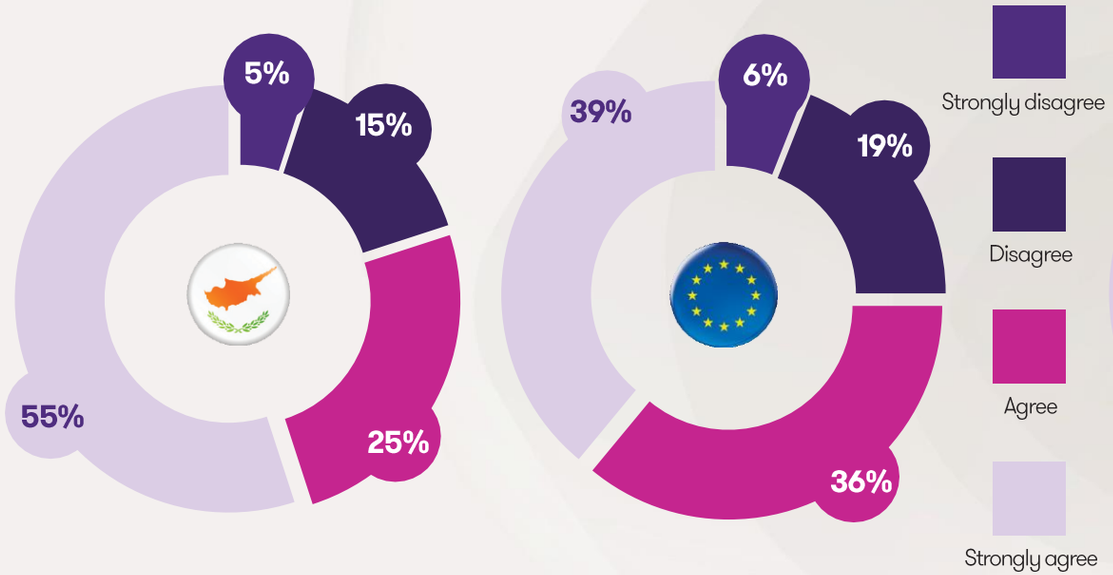


80% of the responders in Cyprus believe that sufficient controls have been defined by their organizations in order to ensure the security of the data. Slightly decreased results have been occurred on a European level where 77% combined of the responders agree on this.

The results are quite satisfactory as they indicate the progress of the organizations towards compliance with the data protection regulation.

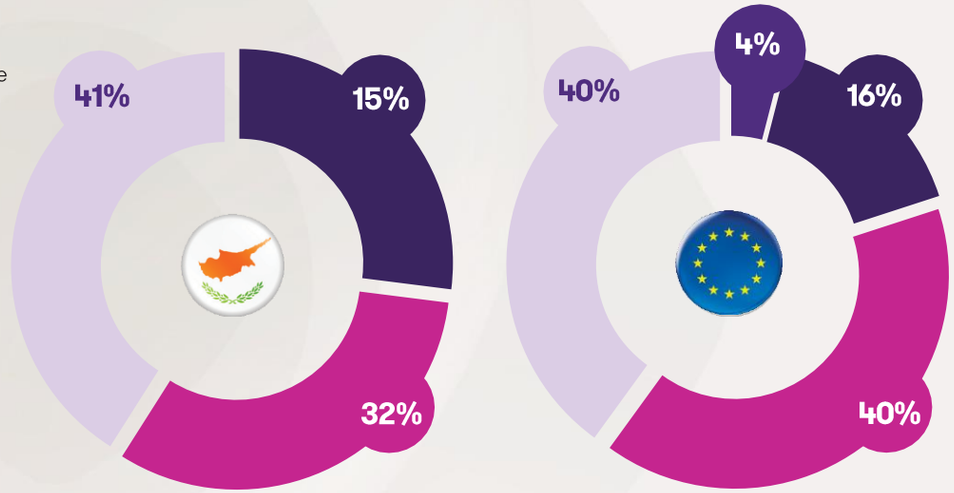
Data breaches and internal awareness

“I am informed of all data breach situations”



Internal communication in relation to data breach is an integral part of compliance with privacy standards and regulation. A combined rate of 80% of the companies in Cyprus are well informed of any data breach incidents whereas a similar rate of 75% stands in Europe.

“Data breach management is functional and works well”



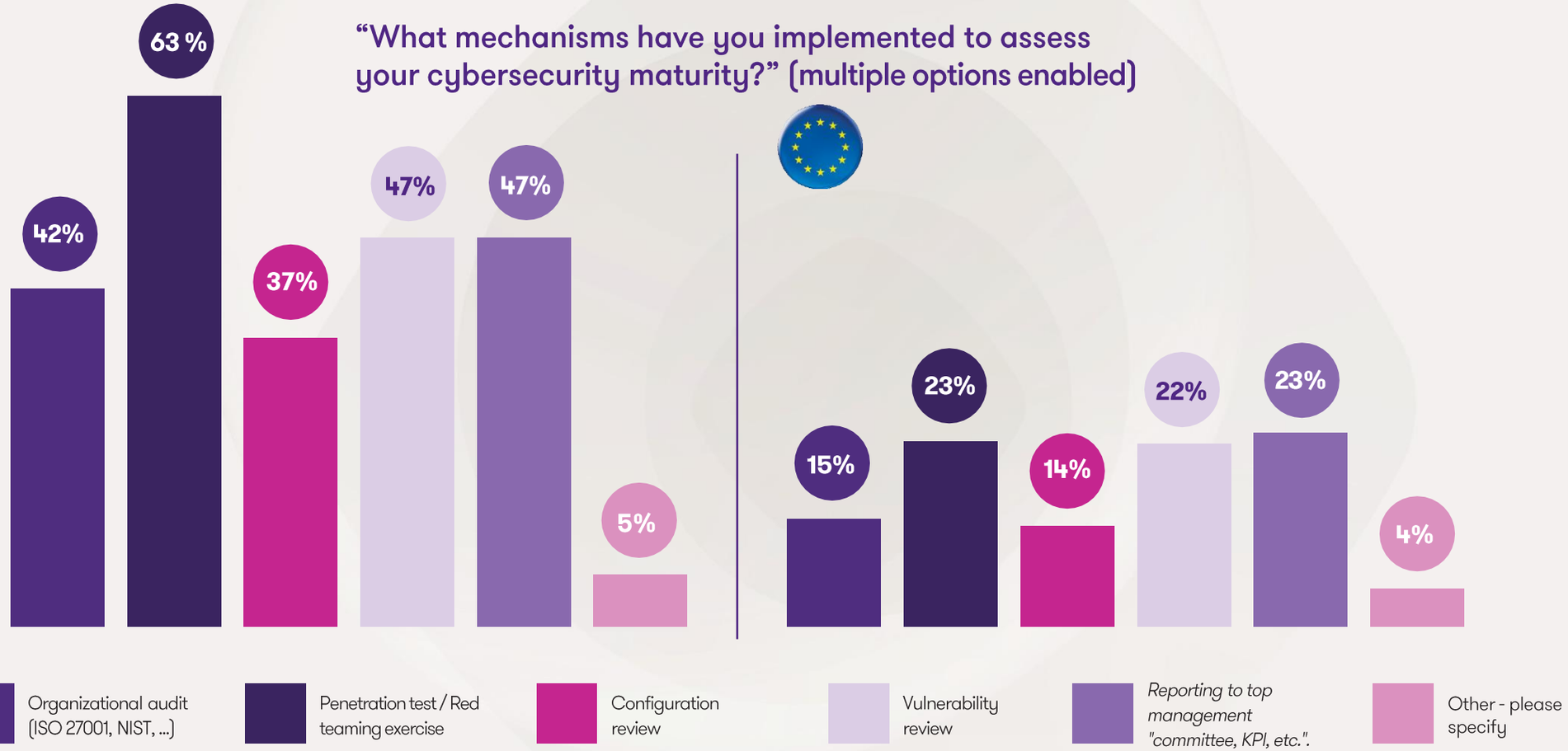
DPOs of companies within Cyprus and Europe, both express their confident that their data breach management procedures work well. More specifically a 41% and 40% respectively strongly agree about the functionality of their data breach procedures.

DPO comments

> **NIS 2 will serve as a lever for us to improve the security of certain parts of the IS.**

Cybersecurity maturity assessment

"What mechanisms have you implemented to assess your cybersecurity maturity?" (multiple options enabled)



Regardless the size of the organizations it has been observed that several mechanisms are utilised to assess the maturity levels of cybersecurity. More specifically 42% of the organizations participated in the survey selected ISO 27001 and NIST as their point of reference for compliance whereas penetration testing was selected by 63% of the companies. Also it has been noted that vulnerability reviews and internal reports to management through committees are also common alternatives to monitor cybersecurity.

These results also demonstrate that the assessment of cybersecurity is rather more technical (penetration testing and vulnerability scanning) than organizational. For an ideal cybersecurity however, the coexistence of both is necessary.

Computer attack simulation exercise

"In the last 12 months, have you carried out an exercise simulating a computer attack involving a leak of personal data?"

It has been occurred that majority of the organizations in Cyprus have not carried out a cyber-attack. More specifically only 35% of the participants have carried out a simulation over the last year.

Response rate on a European level is more satisfactory. However, it remains below of what is expected to guarantee good resilience against cyber-attacks. This good practice should be carried out at least annually by all organizations who have set up a digital infrastructure.

Assessment of subcontractors' cybersecurity

"Within the next 3 months, will you assess your providers/subcontractors on cybersecurity issues?"

In Cyprus, 55%% of the survey responders have not planned to evaluate their service providers on the cybersecurity aspect. **On this point, Cyprus is behind European practices.**

Organizations should assess their subcontractors' readiness towards cybersecurity and ensure that appropriate technical and organisational measures have been implemented in line with best practices since they act on behalf of the organizations.

What you must remember

In light of major IT developments in companies such as the use of artificial intelligence, the DPO remains the safeguard when it comes to data protection.

The DPO can rely on a very good relationship with other information security players such as the CISO.

This will be useful for the projects to be carried out, in particular that of the operational deployment of security measures. Indeed, the concern of DPOs about the general level of data security is coupled with the difficulties on conducting PIAs and reflects this state of affairs.

Despite the fact that DPOs are aware of internal data breaches, companies should continue raising awareness among internal stakeholders.

Measures in place in order to ensure the integrity and confidentiality of data are mainly technically however organizational safeguards play a vital role on the data protection and the overall information security.

It appears from the survey that the most utilised mechanisms are:

- ✓ Performance of penetration tests to identify technical gaps within information systems
- ✓ Vulnerability reviews
- ✓ Reporting to top management and utilisation of KPIs in order to ensure optimal monitoring and to provide reasonable assurance regarding the level of security of information systems

Data security controls must be considered by the DPO and the CISO in order to ensure an adequate level of security. To do this, cyber-attack simulations, third-party security audits and internal organizational audits could provide a cross-functional vision and usefully complement the technical with organizational measures.

Subsequently, faced with a new era of digitalization, the CISO / DPO tandem remains essential to ensure the overall compliance of the organizations with data protection regulations and information security standards.

06 Conclusion

Conclusion

In Cyprus, organizations have been diligently working to align with GDPR requirements over the last years, including the appointment of DPOs where necessary. Many large enterprises and public sector entities have designated DPOs to fulfil their obligations under the regulation. However, compliance varies across sectors and sizes of the organizations.

The significance of investing in data protection, has been already perceived in certain industries. Nevertheless, a considerable percentage of organizations undervalue this aspect. Additional and consistent effort is needed to embed data protection and safeguard of privacy within the corporate culture irrespective of the business industry an entity operates.

While there has been progress within Cyprus and EU on implementing compliance measures, continuous efforts are necessary to tackle the evolving nature of data protection regulations. The role of a DPOs is pivotal in ensuring adherence to the responsibilities of their organizations under the GDPR, and their role should not be underestimated by the managements. By investing in resources and promoting collaboration, organizations in Cyprus can enhance their data protection endeavours and cultivate trust with data subjects and regulatory authorities alike.

Stavros Demetriou

Manager, Digital Risk

Grant Thornton Cyprus

Grant Thornton Cyprus

Grant Thornton Cyprus is one of the leading professional services firm in the country. We offer a full range of assurance, tax, specialist advisory and outsourcing services to clients – ranging from public companies and multinationals to private business across a broad spectrum of industries.

We pride ourselves on having partner-led services for all our clients. We combine excellent technical knowledge with the intuition, insight and confidence gained from our extensive sector experience and a deep understanding of our clients.

2
Offices
Nicosia & Limassol

170+
People with **62% of women** across all levels

17
Partners and Directors with nearly **40% of women** at partner level

Our services

Assurance
Tax & VAT
Advisory
Digital Risk
Insolvency & Asset Recovery
Distributed Ledger Technologies
Business Consulting
Outsourcing
Quantitative Risk
ESG & Sustainability
Risk & Compliance
Regulatory Compliance & Funds

Nicosia office, Headquarters

41-49 Agiou Nicolaou Street
Nimeli Court, Block C, 2408
Engomi. P.O.Box 23907
1687 Nicosia
Cyprus

Tel: +357 - 22600000

Limassol office

143, Spyrou Kpyrianou Avenue
Chrysanthou Business C
P.O.Box 56513, 3307
Limassol
Cyprus

Tel: +357 - 25248000