GDPR

COMPLIANCE IN THE EU

LinkedIn Group Partner
Information Security

ALERT LOGIC®
Security. Compliance. Cloud.

INTRODUCTION

Going into effect in May of 2018, the European Union General Data Protection Regulation (EU GDPR) represents the most sweeping change in data privacy regulation in decades.

EU GDPR imposes strict requirements on all companies that collect and retain personal data of users and customers.

This report conducted during the month of July, 2017 is the result of a comprehensive research study in partnership with the 370,000+ member Information Security Community on LinkedIn and Crowd Research Partners.

This research uncovers the perspectives of organisations located in the European Union on the impact of the new regulations and how they plan to be in compliance with the mandated requirements.

Many thanks to Alert Logic for supporting this exciting research project.

Thank you,

Holger Schulze

Holger Schulze
Founder
Information Security
Community on LinkedIn

hhschulze@gmail.com

LinkedIn Group Partner
Information Security

ALERT LOGIC®

GDPR COMPLIANCE

IN THE EU | 2017 SURVEY

KEY SURVEY FINDINGS

1. While an overwhelming majority of surveyed EU companies are familiar with the EU GDPR regulations, only about a third (33%) state that they are compliant or well on the way to compliance.

2. About a third of EU based companies (32%) expect substantial changes to their company's security practices and technologies in order to become compliant with EU GDPR policies.

3. The biggest challenge in becoming GDPR compliant is lack of budget (50%), closely followed by lack of expertise (48%) and limited understanding of GDPR regulations (37%).

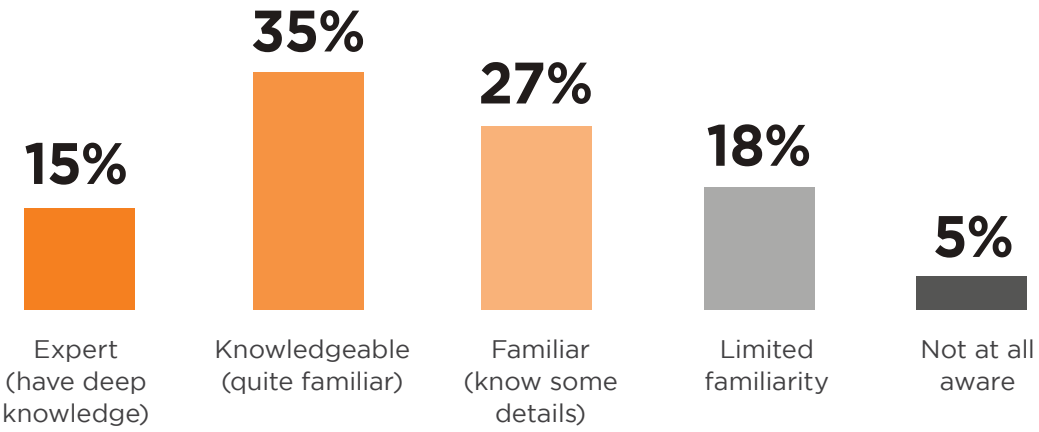
4. Among the many articles of GDPR, EU companies are most concerned about "Data protection by design and by default", likely because it implies significant system re-design and investment in data protection controls and processes.

5. Only 5% of EU companies believe they are in compliance with all applicable GDPR requirements today. 27% are not confident they will meet the deadline.

FAMILIARITY WITH EU GDPR REGULATIONS

Half of the EU respondents have some or deep knowledge about the GDPR regulation while 45% have only low levels of familiarity with the law.

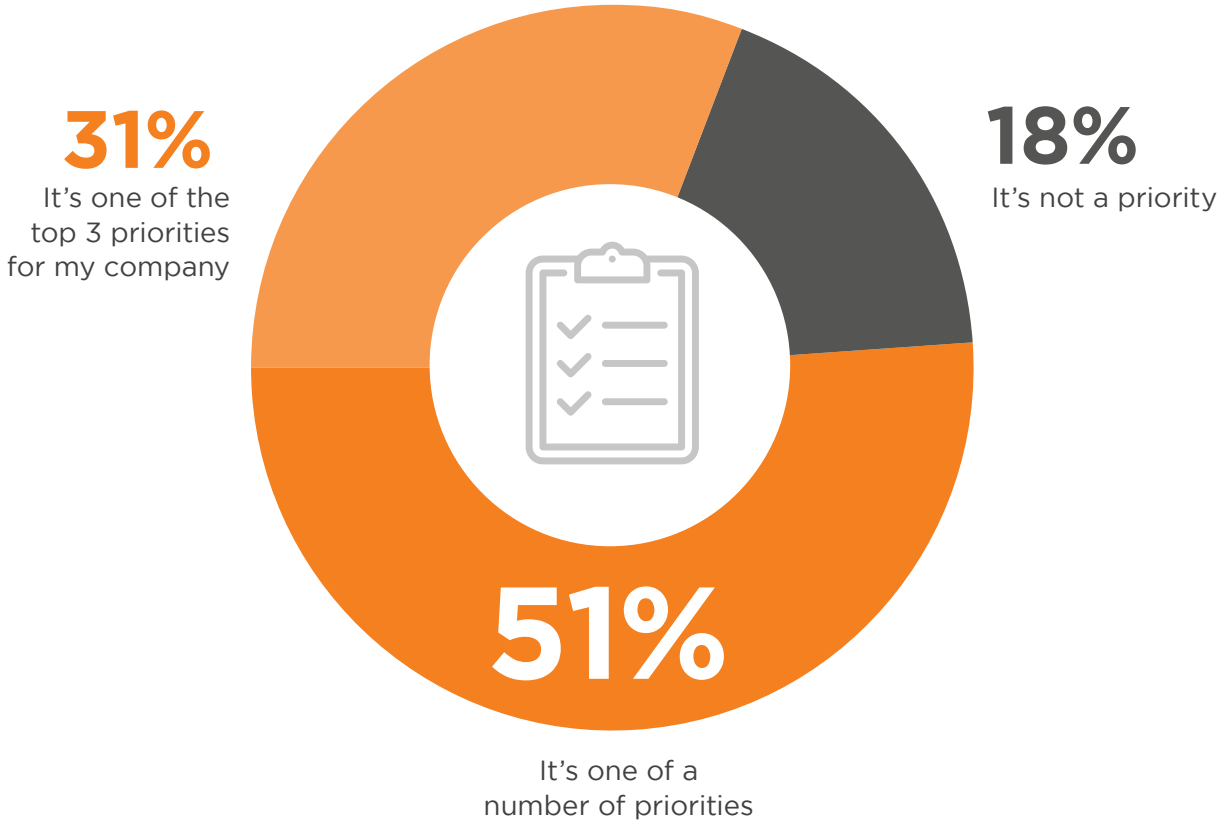
Q: How familiar are you with the EU GDPR?



COMPLIANCE PRIORITY

GDPR compliance is a priority for the vast majority of respondents (82%), on the other hand 18% say it isn't a priority - but that won't exonerate them from compliance to it. For about a third (31%) it is one of their company's top three priorities.

Q: How high of a priority is EU GDPR compliance to your company currently?



GDPR PREPAREDNESS

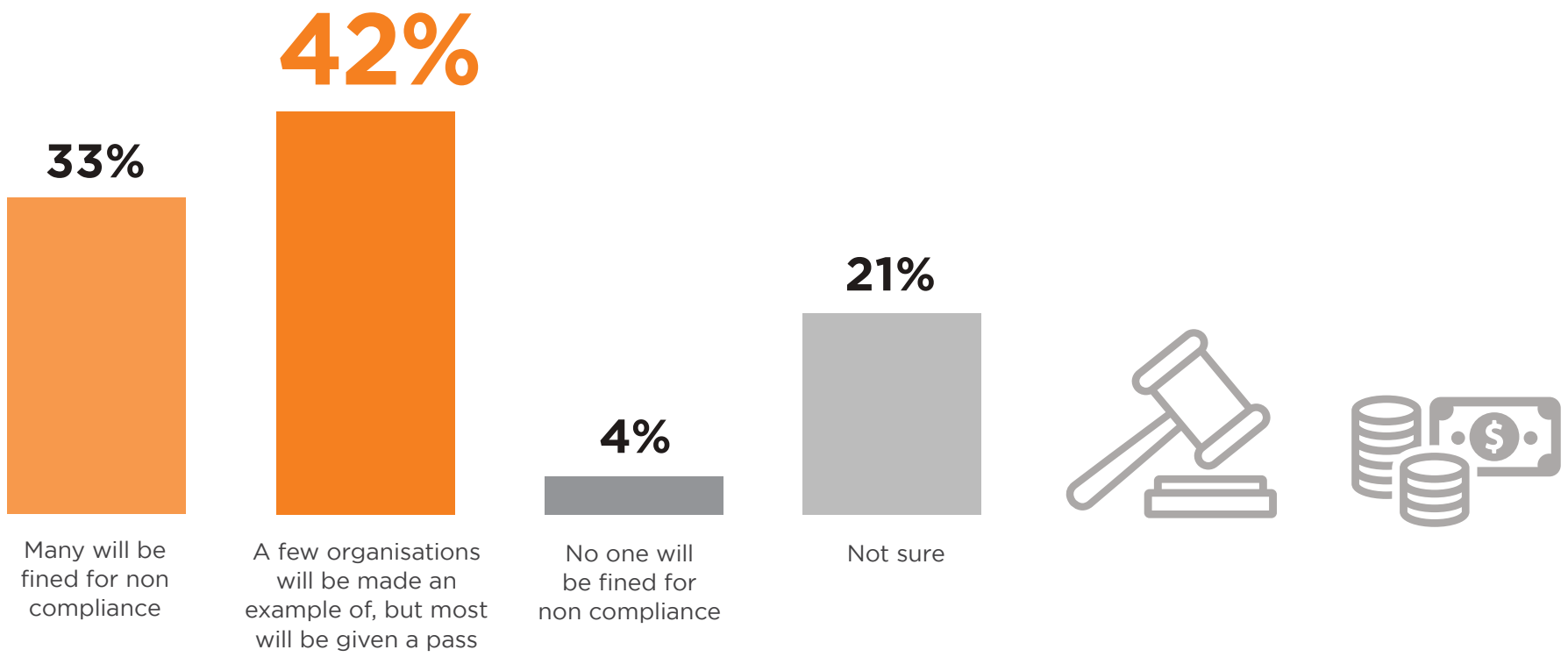
Only 5% of companies in our survey believe they are in compliance with all applicable GDPR requirements today. 27% are not confident they will meet the deadline. Not coincidentally, organisations where EU GDPR compliance is a high priority are further ahead in the process of becoming compliant.

Q: How prepared is your company to meet EU GDPR regulations by the deadline of May 25, 2018?

REGULATORY ENFORCEMENT

A third of organisations expect that the regulators will issue a significant amount of fines due to companies found to be non compliant. 42% expect only a few organisations will be made an example for non compliance.

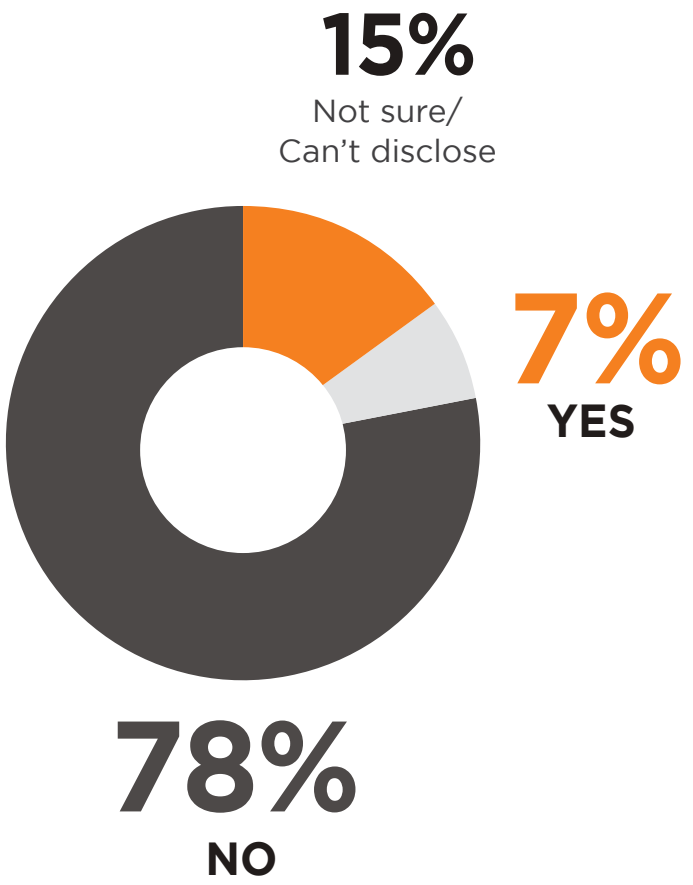
Q: How strictly do you believe the EU GDPR regulation will be enforced when it officially comes into effect?



REGULATORY SANCTIONS

Only a small portion of organisations confirm they have been subject to regulatory fines or sanctions in the past five years.

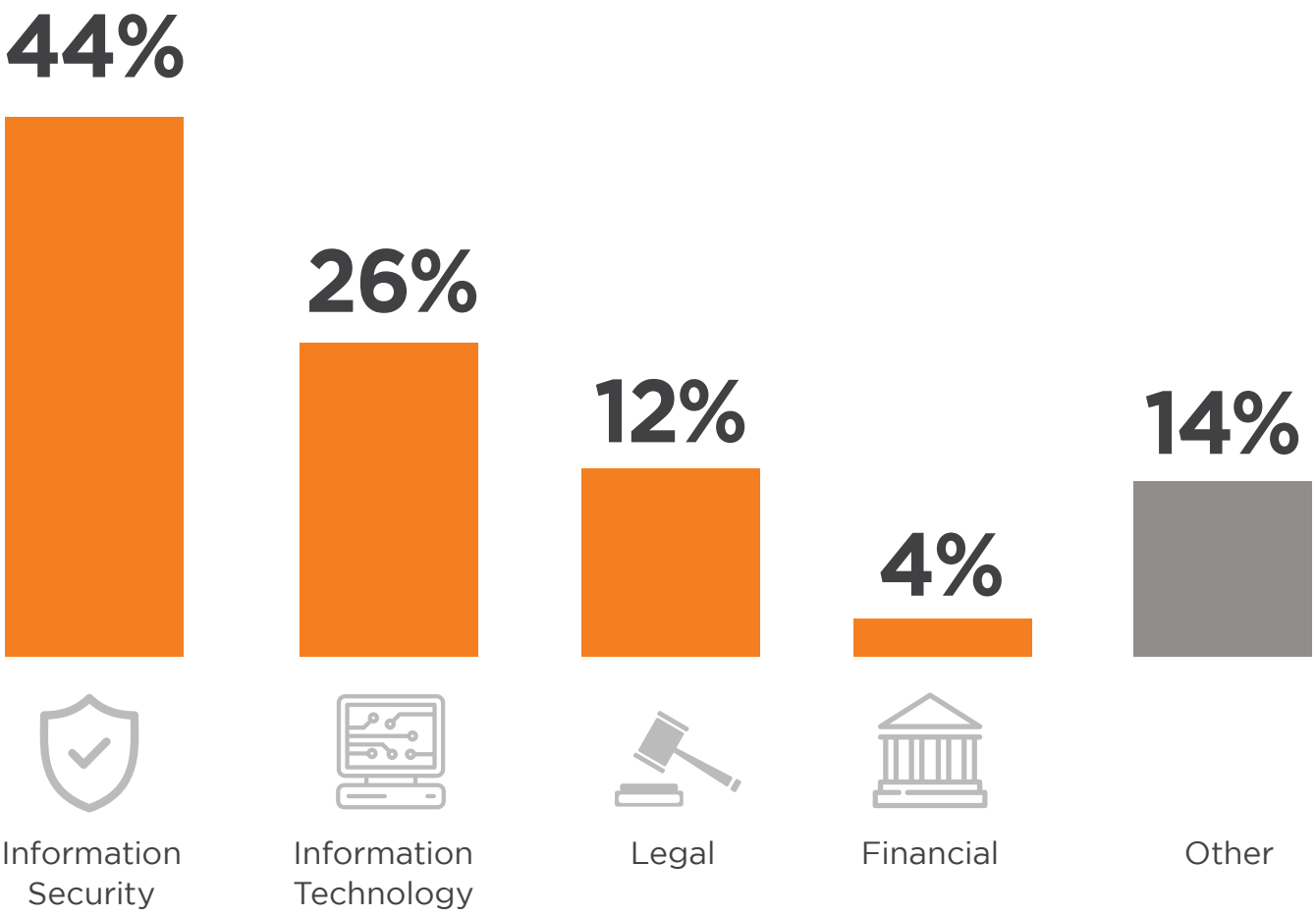
Q: Has your company faced any regulatory sanctions in the past 5 years?



ORGANISATIONAL OWNERSHIP

In most organisations, Information Security teams have primary ownership for meeting EU GDPR compliance (44%). This is especially true for companies where compliance is a top priority.

Q: What team within your company has primary responsibility for ensuring EU GDPR compliance?



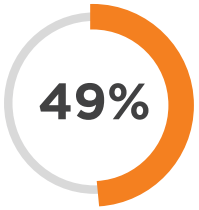
COMPLIANCE INITIATIVES

A majority of respondents (80%) indicate that making an inventory of user data, and mapping the data to protected EU GDPR categories, is a key initiative in their GDPR compliance programs.

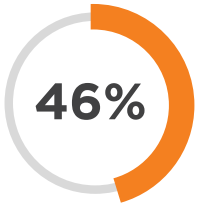
Q: Which of the following initiatives are part of your program to be compliant with EU GDPR regulations?

80% Making an inventory of user data and mapping to protected EU GDPR categories

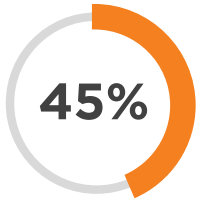
Evaluating solutions to enable users to exercise their data rights



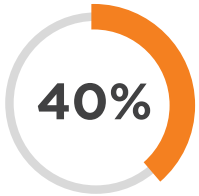
Designing applications and databases to have default data privacy enabled



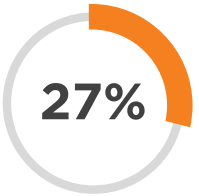
Audit to track down "rogue" data records with personal information



Identify and integrate internally developed solutions



Identify and integrate external applications

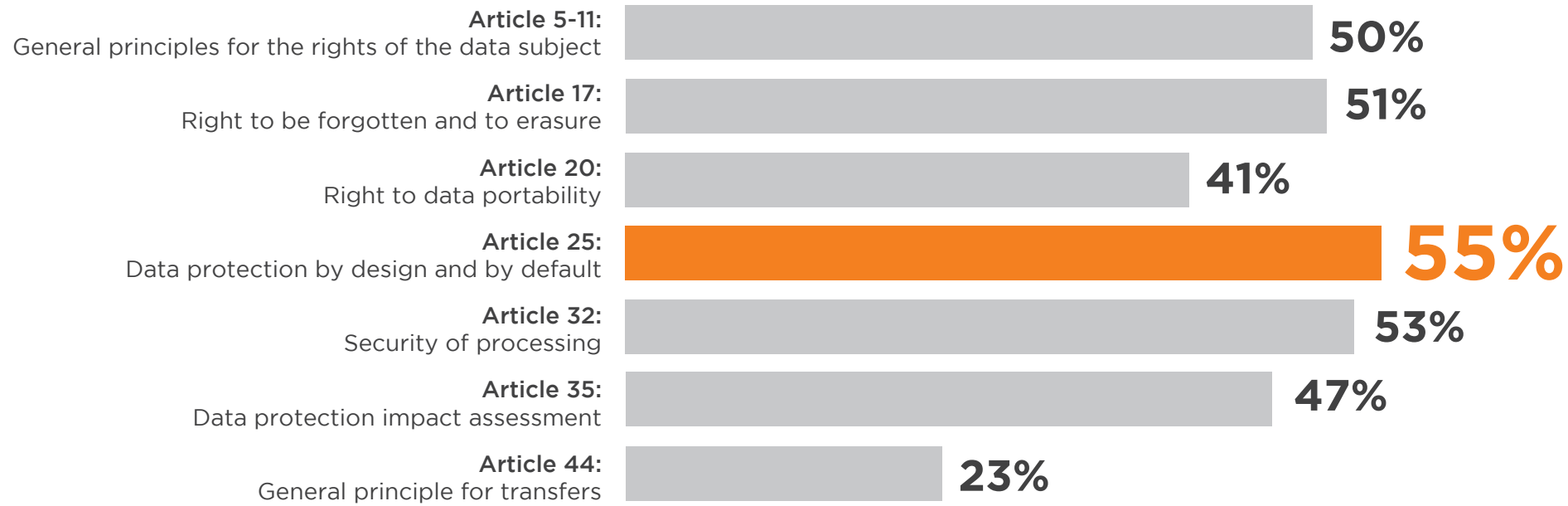


Stress-testing resilience of proposed GDPR solutions

GDPR ARTICLES OF CONCERN

Among the many articles of EU GDPR, of significant concern to EU companies is "Data protection by design and by default", likely because it implies significant system re-design and investment in data protection controls and processes.

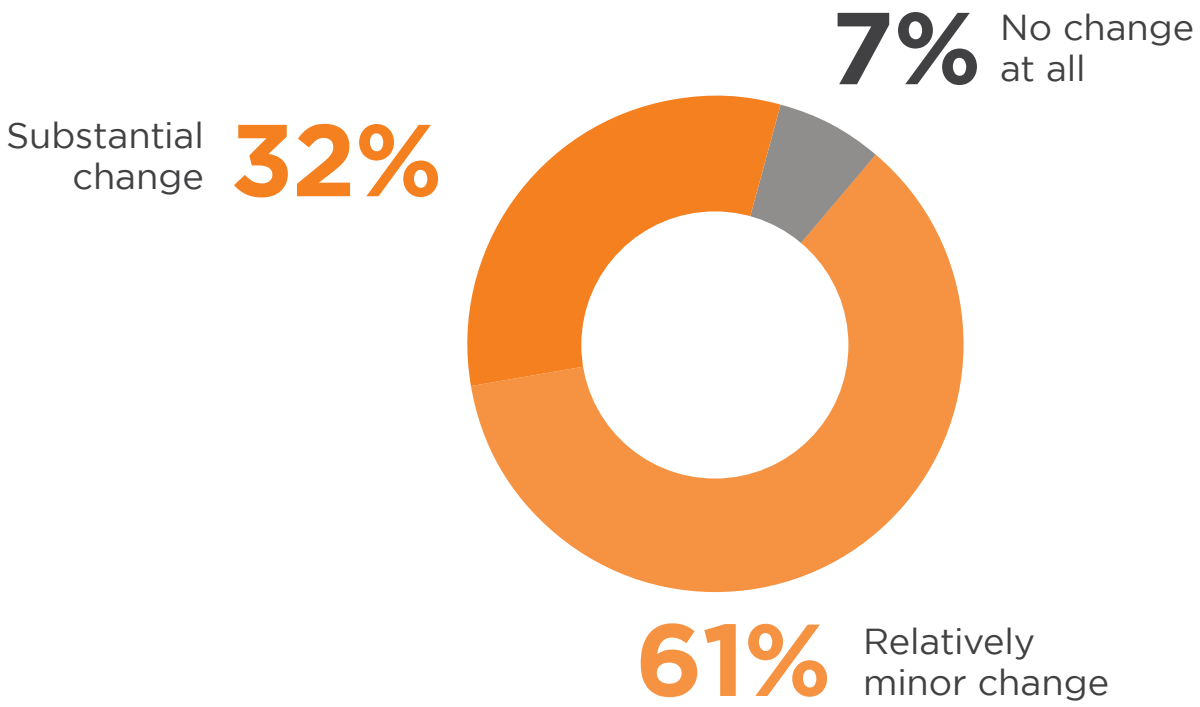
Q: Which of the following provisions are of the most concern to you?



IMPACT ON SECURITY PRACTICES

About a third of EU based companies (32%) expect substantial changes to their company's security practices and technologies in order to be in compliance with EU GDPR policies.

Q: To what level will your company's security practices and technology need to change to be in compliance with EU GDPR policies?



COMPLIANCE CHALLENGES

The most frequently mentioned challenge in becoming GDPR compliant is lack of budget (50%), closely followed by lack of expertise (48%) and limited understanding of GDPR regulations (37%).

Q: What challenges is your company facing in becoming compliant with EU GDPR regulations?

50% **#1** Lack of budget

#2 48% Lack of expert staff with critical skills

#3 37% Limited understanding of regulations

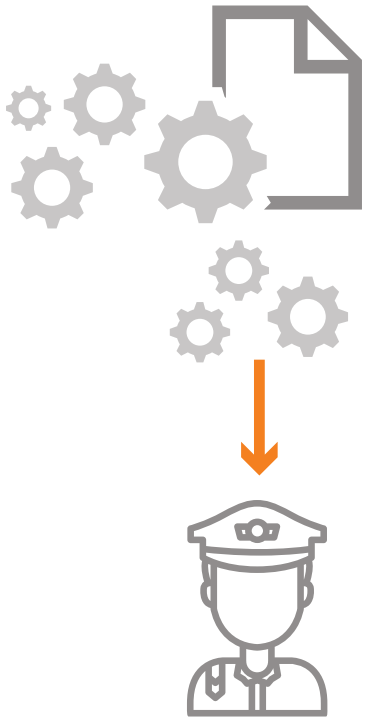
#4 32% Lack of management support

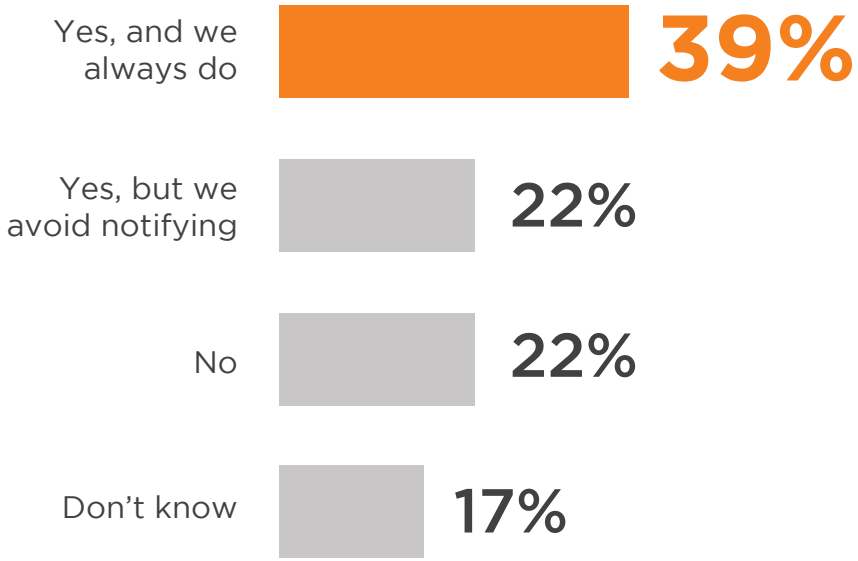
#5 29% Lack of necessary technology

DATA BREACH PROCESS

A majority of EU companies (61%) has a formal process in place to notify authorities in the event of a data breach. Only 39% of organisations confirm they always follow this process.

Q: Does your business have a formal process in place to notify the data protection authority within 72 hours in the event of a data breach?





BIGGEST DATA THREAT

EU based companies see cyber criminals as the biggest threat to sensitive data (83%) followed by accidental loss through employees (61%) and deliberate theft by employees (30%).

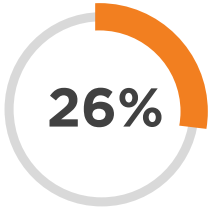
Q: : Which of the following do you see as the biggest threat to your data?

83%
Cyber criminals

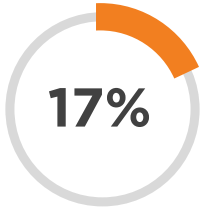
61%
Accidental loss by employees

30%
Deliberate threat by employees

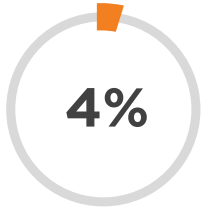
Customers



Government



Competitors



Other

METHODOLOGY AND DEMOGRAPHICS

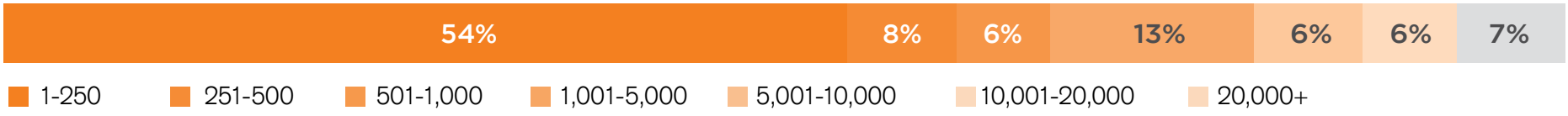
METHODOLOGY & DEMOGRAPHICS

The 2017 EU GDPR Report is based on the results of a comprehensive online survey of over 200 EU based companies conducted in July 2017.

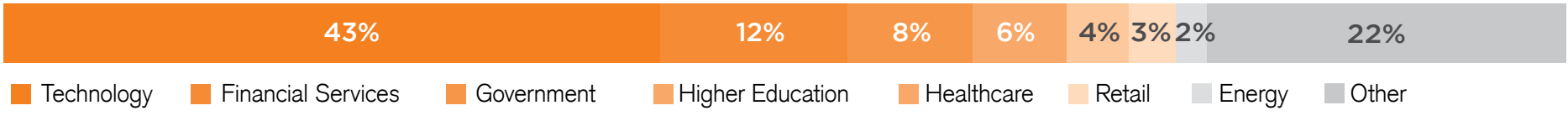
CAREER LEVEL

DEPARTMENT

COMPANY SIZE



INDUSTRY



WHERE TO START

1. Understanding where your data is:

This is one of the critical areas to securing your data, once you know where your data is, it is important for GDPR that you have a legal basis to collect this information.

2. Identifying the potential threat:

The next step is to scan your systems for vulnerabilities to identify if there are any areas that could increase the risk of compromise.

3. Protecting your server environment:

Once you understand your attack surface area, you need to ensure you have visibility of attacks at the application, operating system and network layer. In order to respond fast and address the 72-hour response time, visibility is critical.

4. Protecting your application workloads:

The #1 attack vector is applications, several breach examples today are due to the exploitation of exposed applications.

Alert Logic Supports GDPR by allowing you to:

Continuous reporting on vulnerabilities and configuration flaws in your cloud workloads.

Alert Logic provides incident escalation and remediation guidance – within 15 minutes! GDPR stipulates the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Attack filtering logic turned specifically for each environment. We identify, verify, escalate the security risks that could threaten your infrastructure, and recommend the best course of action to remediate and neutralize the situation. It also includes a knowledge base for remediation steps and creates an incident audit trail for auditors and regulators.

Log security monitoring, daily review and archive is provided to detect attacks and provide evidence for the regulators that you understand the threat.

CONTACT US

Resources Available To You

Let Alert Logic keep you up-to-date of the latest developments in the cloud security industry – from emerging security threats to the most recent changes in compliance regulations through a variety of resources including:

Alert Logic Weekly Threat Report

Subscribe to receive a weekly email of the three biggest breaches of the week from around the globe and the Top 20 malicious IP addresses.

https://www.alertlogic.com/resources/threat-reports/

Alert Logic Blog

Subscribe to our blog which provides commentary on topics that are related to our technologies and industry topics.

https://www.alertlogic.com/resources/blog/

On-Demand Webinar

GDPR: Ready or Not, Here it comes

https://www.alertlogic.com/resources/webinars/gdpr-ready-or-not,-here-it-comes/

ALERT LOGIC®

U.S. 877.484.8383 | U.K. +44 (0)203 011 5533
INFO@ALERTLOGIC.COM | ALERTLOGIC.COM