2018

GDPR COMPLIANCE REPORT

Cybersecurity INSIDERS

Crowd Research Partners

ALERT LOGIC®

INTRODUCTION

Effective as of May 25, 2018, the European Union General Data Protection Regulation (GDPR) represents the most sweeping change in data privacy regulation in decades.

GDPR imposes strict requirements on how consumer data is collected, used, and stored, including U.S. companies doing business in EU countries.

Security breaches must be immediately disclosed, explicit consent for data collection is required, and users have the right to full erasure of data - with all costs for technology, people, and processes carried by the entity collecting the data.

This report is the result of a comprehensive research study commissioned by Cybersecurity Insiders in partnership with the 400,000+ member Information Security Community on LinkedIn to provide clarity on the state of GDPR compliance.

This research uncovers the perspectives of organizations on the impact of the new regulation, how prepared they are, and how they plan to be in compliance with the new law to avoid significant penalties.

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

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

Holger.Schulze@Cybersecurity-Insiders.com

KEY SURVEY FINDINGS

1. A whopping 60% of organizations are at risk of missing the GDPR deadline. Only 7% of surveyed organizations say they are in full compliance with GDPR requirements today, and 33% state they are well on their way to compliance deadline.

2. While 80% confirm GDPR is a top priority for their organization, only half say they are knowledgeable about the data privacy legislation or have deep expertise; an alarming 25% have no or only very limited knowledge of the law.

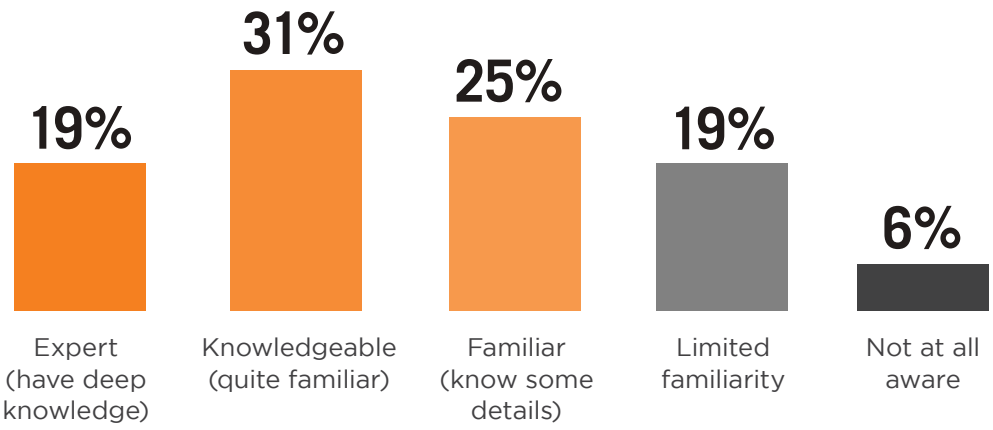
3. The primary compliance challenges are lack of expert staff (43%), closely followed by lack of budget (40%), and a limited understanding of GDPR regulations (31%). A majority of 56% expect their organization's data governance budget to increase to deal with GDPR challenges.

4. Approximately a third of surveyed companies report that they will need to make substantial changes to data security practices and systems to be in compliance with GDPR. The highest ranked initiative for meeting EU GDPR compliance is to make an inventory of user data and map it to protected EU GDPR categories (71%), followed by evaluating, developing, and integrating solutions that enable GDPR compliance.

FAMILIARITY WITH GDPR REGULATIONS

Half of respondents have some or deep knowledge about the GDPR regulation. An alarming 25% have no or only very limited knowledge of the the law.

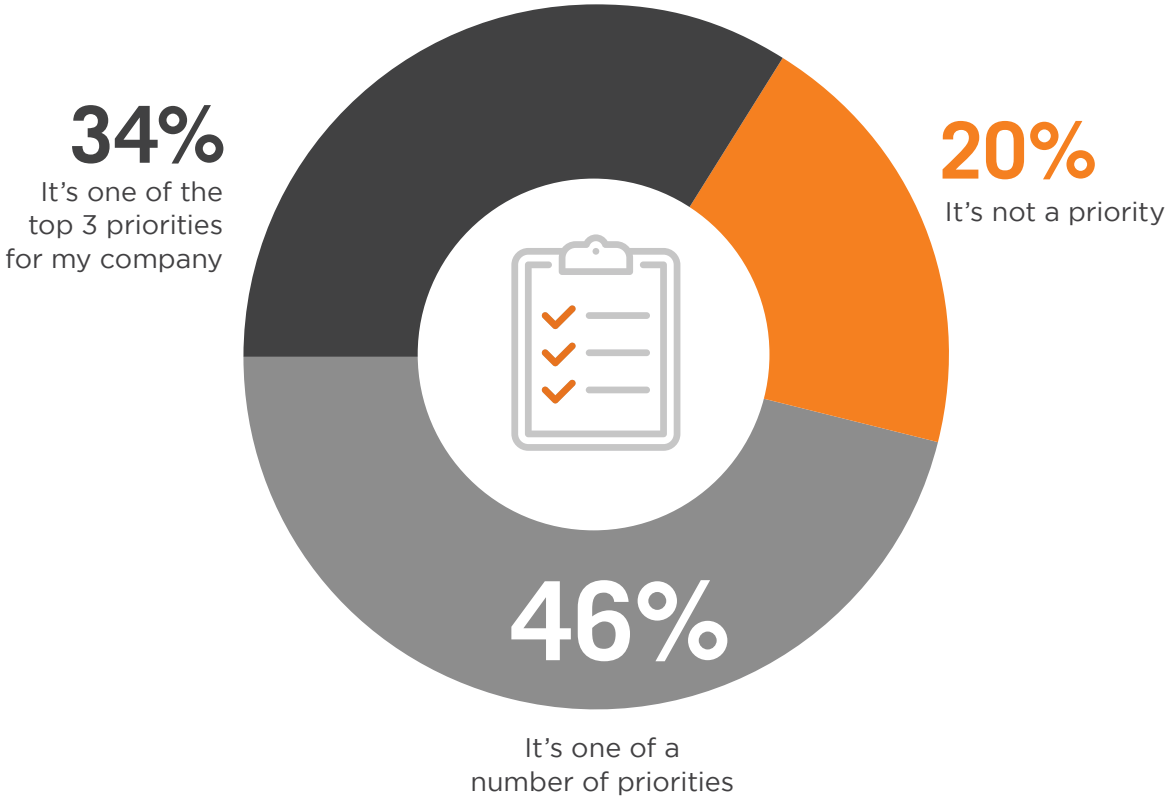
How familiar are you with GDPR?



COMPLIANCE PRIORITY

GDPR compliance is a priority for the vast majority of respondents (80%); for a third of respondents (34%) it is one of the top three priorities. 20% say GDPR isn't a priority - but that won't relieve them from having to comply with the law.

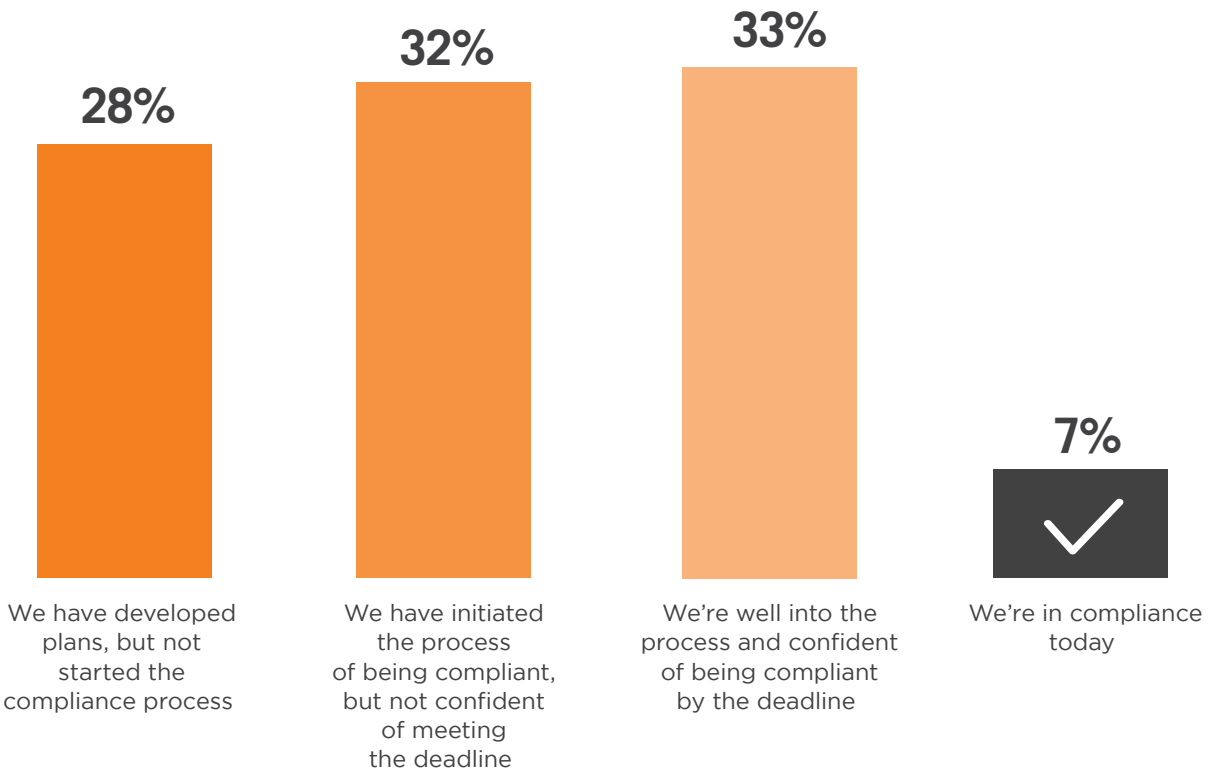
How high a priority is GDPR compliance to your company?



GDPR PREPAREDNESS

Only 7% of companies in our survey believe they are in compliance with GDPR requirements today. While this is an improvement over last year's survey results where only 5% indicated compliance readiness - it is still an alarmingly low number. A third of companies (33%) are on their way to compliance; they are confident they will meet all requirements by the deadline. A whopping 60% of organizations are at risk of missing the compliance deadline.

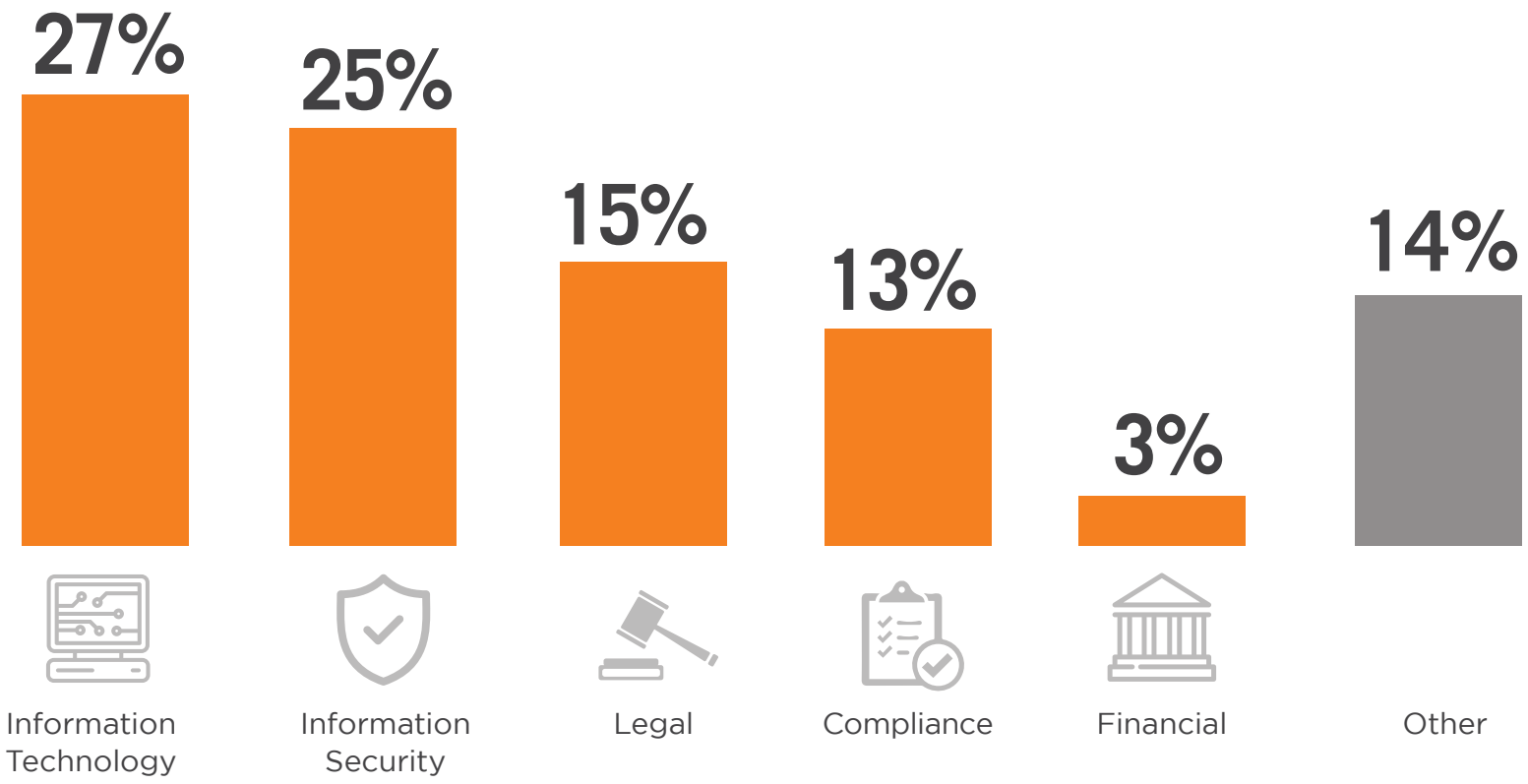
How prepared is your company to meet EU GDPR regulations by the deadline of May 25, 2018?



ORGANIZATIONAL OWNERSHIP

In most organizations, IT (27%) and Information Security (25%) teams have primary ownership for meeting GDPR compliance (52%).

What team within your company has primary responsibility for GDPR compliance?

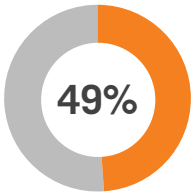


COMPLIANCE INITIATIVES

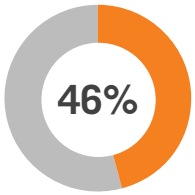
A majority of respondents (71%) indicate that making an inventory of user data, and mapping the data to protected GDPR categories, is a priority initiative in their GDPR compliance programs. This is followed by evaluating, developing, and integrating solutions that enable GDPR compliance.

Which of the following initiatives are part of your GDPR compliance program?

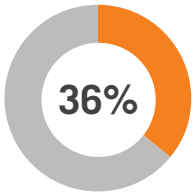
71% Making an inventory of user data and mapping to protected EU GDPR categories



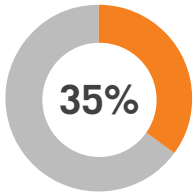
Evaluating solutions to enable users to exercise their data rights



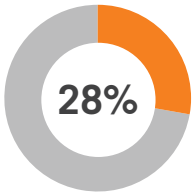
Designing applications and databases to have default data privacy enabled



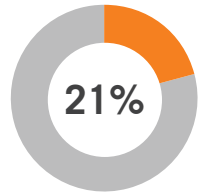
Identify and integrate internally developed solutions



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



Identify and integrate external applications



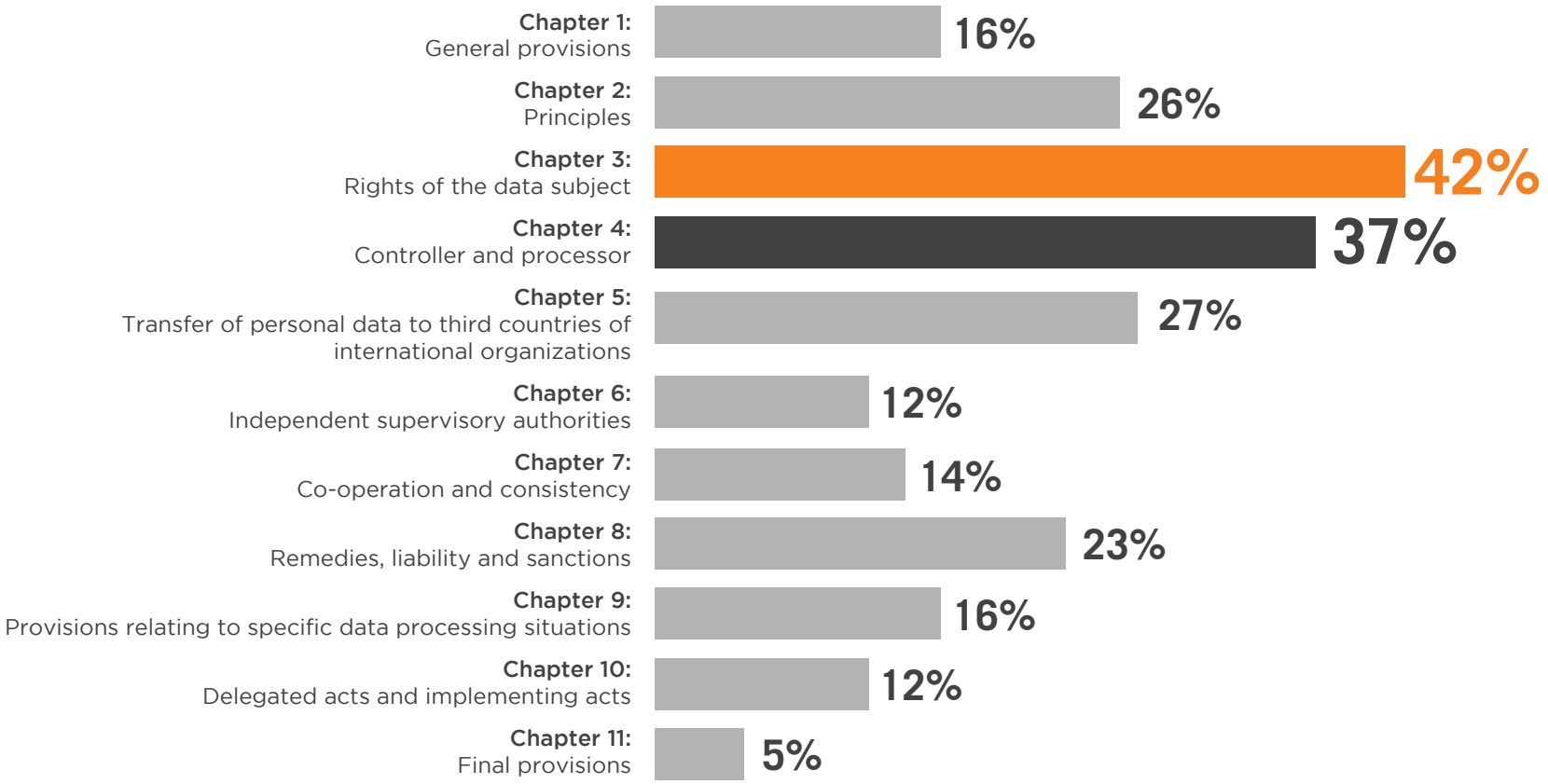
Stress-testing resilience of proposed GDPR solutions

Other 10%

GDPR CHAPTERS IN FOCUS

Among the eleven chapters making up GDPR regulation, survey participants are most concerned about implementing chapter 3, focused on the rights of the data subject, which is at the core of GDPR regulations to protect EU citizens data privacy.

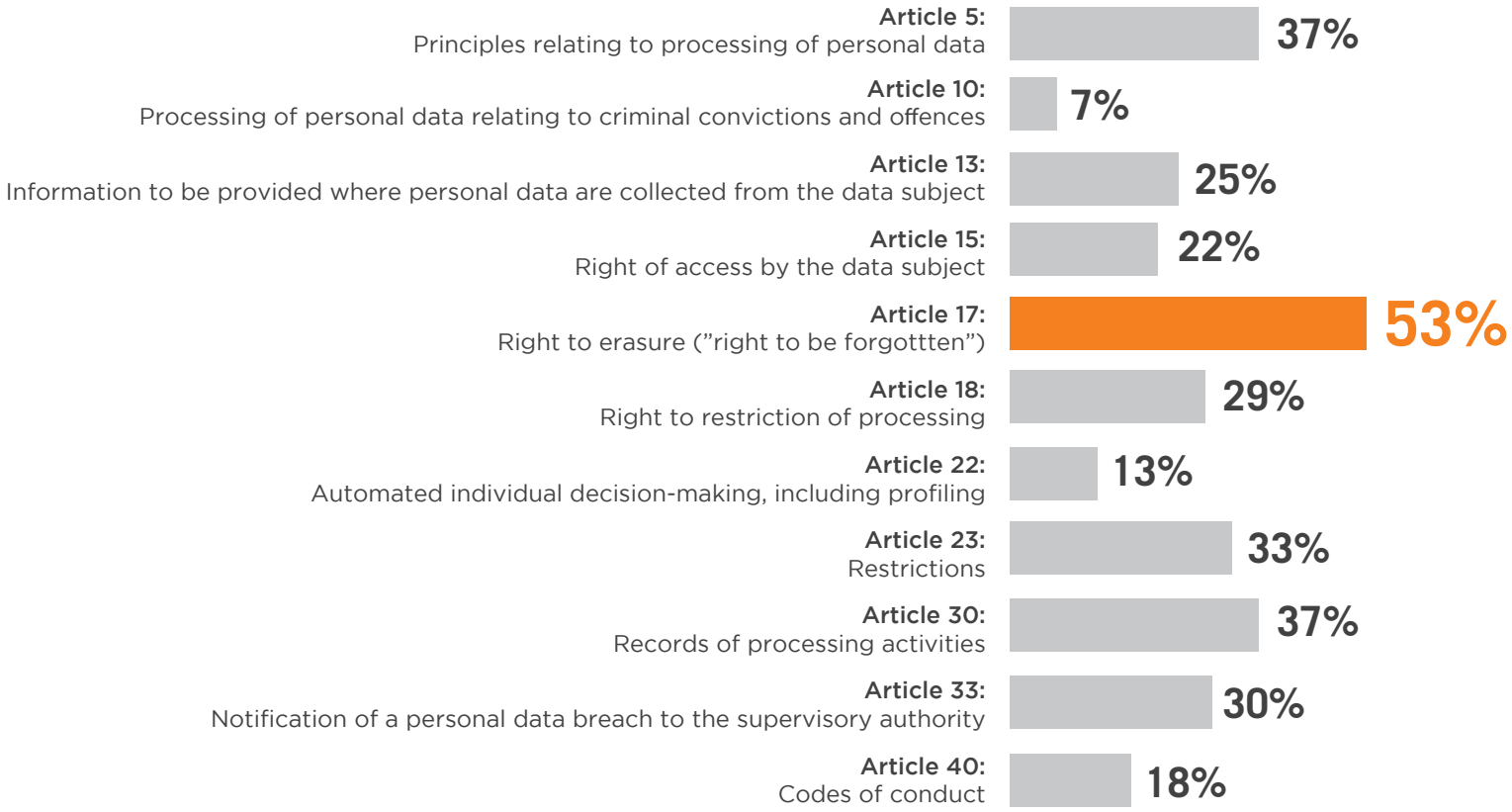
Our GDPR compliance program is most concerned about the following GDPR chapters:



GDPR ARTICLES OF CONCERN

Among the many articles that make up the GDPR legislation, the right to be forgotten and erasure (article 17) and secure processing of personal data (article 30 and article 5) rank as the highest concerns. This is likely because these requirements imply significant system re-design and investment in data protection controls and impact on business processes.

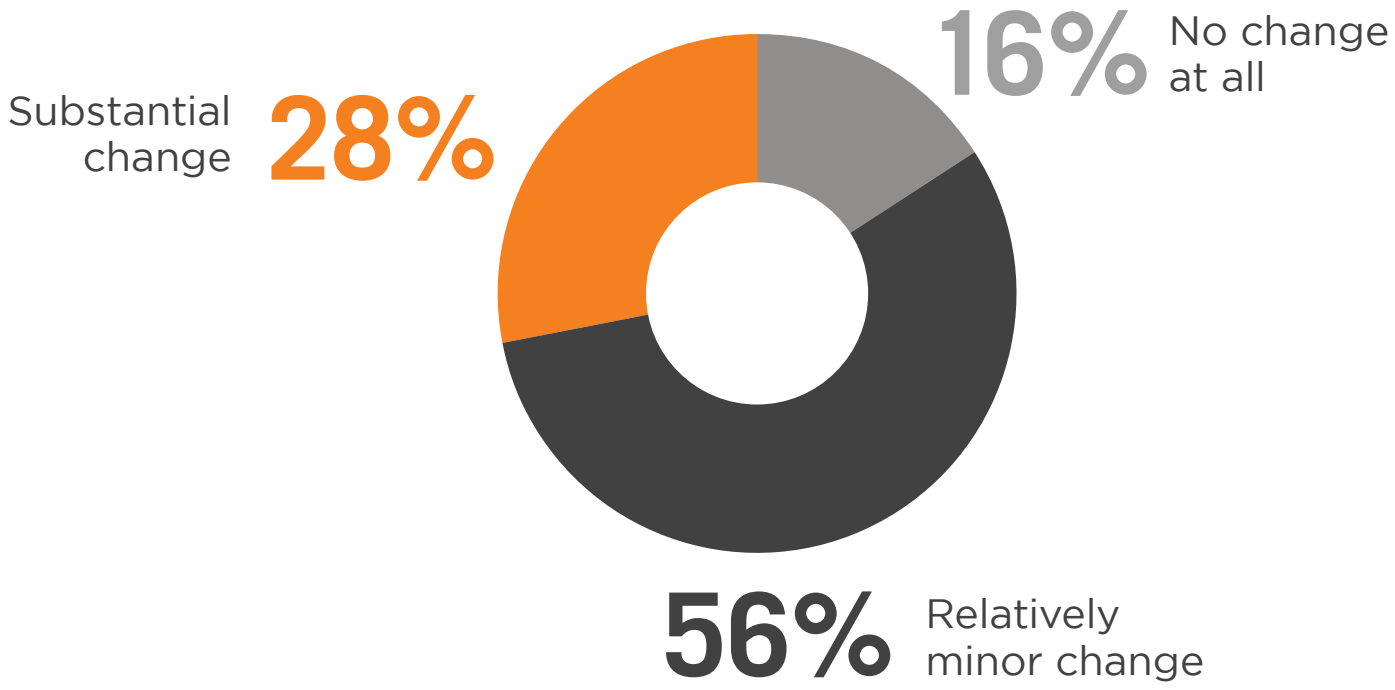
Which of the following provisions are of the most concern to you?



IMPACT ON SECURITY PRACTICES

About a third of companies (28%) expect substantial changes to their security practices and systems in order to be in compliance with GDPR policies. A majority of 56% expect only minor changes.

How significant will be the changes to your company's security practices and technology to be in compliance with GDPR?



COMPLIANCE CHALLENGES

The most frequently mentioned challenge in becoming GDPR compliant is lack of expert staff (43%), closely followed by lack of budget (40%), and a limited understanding of GDPR regulations (31%).

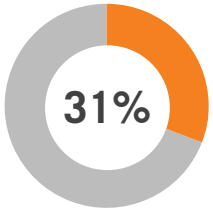
What challenges are your company facing in becoming compliant with GDPR regulations?

43%

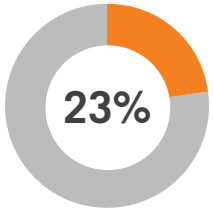
Lack of expert staff with critical skills

40%

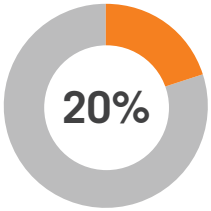
Lack of budget



Limited understanding of regulations



Lack of necessary technology



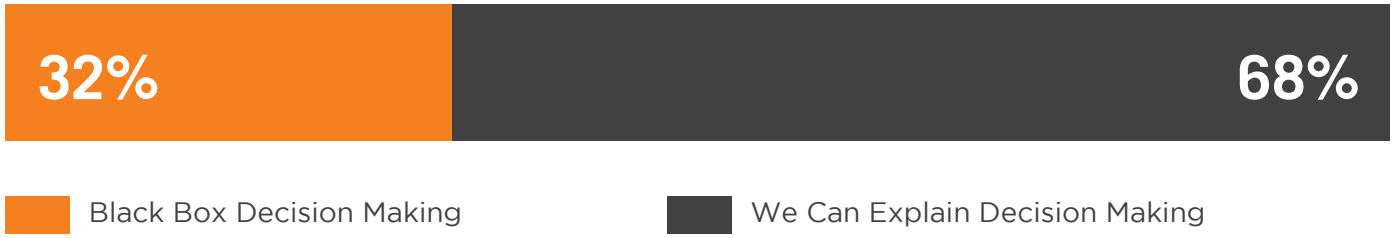
Lack of management support

Other 12%

INSIDER THREAT PROGRAM COMPLIANCE

Most organizations' insider threat programs are currently not meeting GDPR reporting guidelines (56%). The law's 'Right to Explanation' provides citizens the right not to be subject to a decision based solely on automated processing. A third of organizations (32%) confirm their current automated assessment techniques are 'black boxed' meaning they are not able to explain how the algorithms made a decision.

Does your current Insider Threat program currently meet GDPR reporting guidelines?

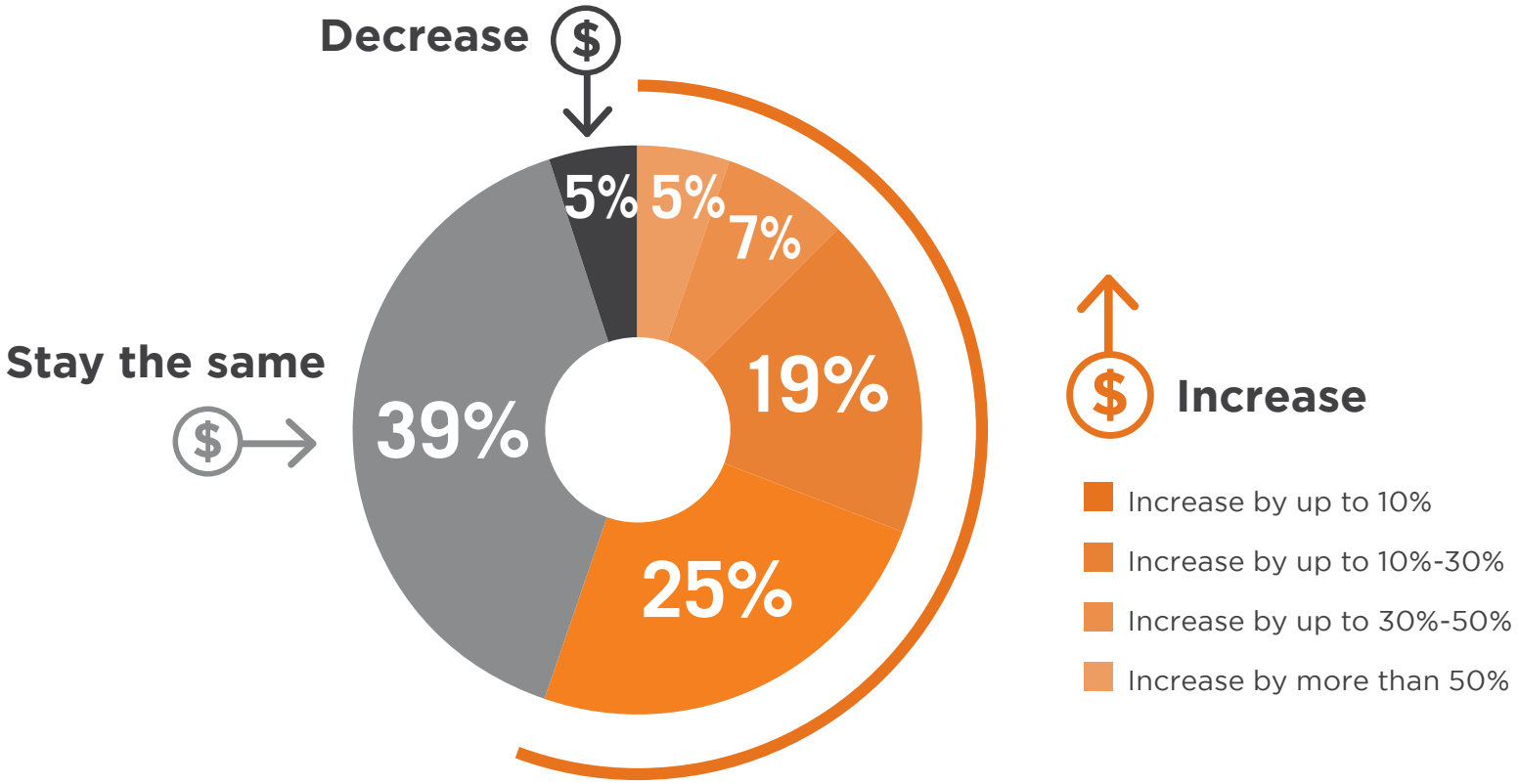


Are your current automated assessment techniques 'black boxed' or are you able to explain how the algorithms made a decision?

DATA GOVERNANCE BUDGET

A majority of 56% expect their organization's data governance budget to increase. 39% expect budgets to stay flat, and only 5% foresee a decline.

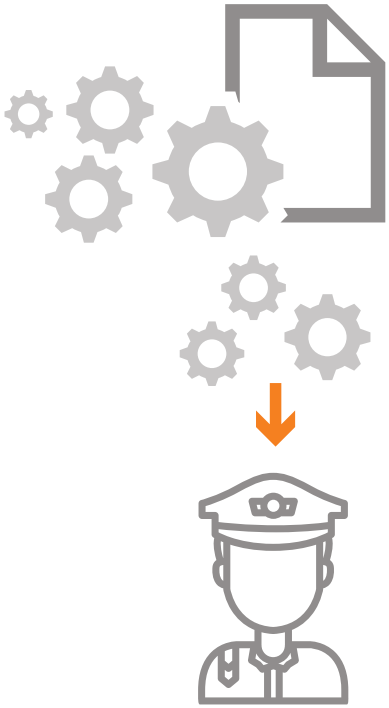
Over the next 12 months, our company's data governance budgets will …

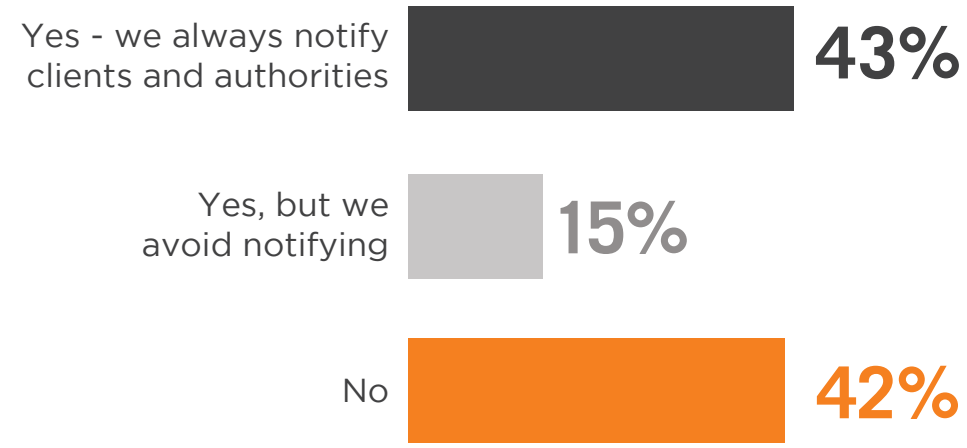


DATA BREACH NOTIFICATION

A majority of companies (58%) have a formal process in place to notify authorities in the event of a data breach (Article 33). However, only 43% of organizations confirm they always follow this process.

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

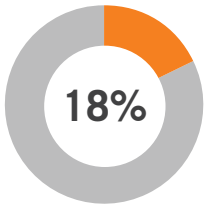
The surveyed companies see cyber criminals as the biggest threat to sensitive data (60%), closely followed by accidental loss through employees (57%), and deliberate theft by employees (30%).

What groups pose the biggest threat to your organization's data?

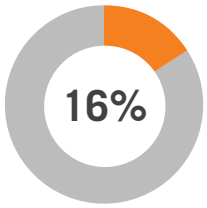
60%
Cyber criminals

57%
Accidental loss by employees

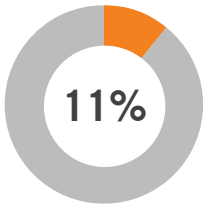
30%
Deliberate theft by employees



Customers



Competitors



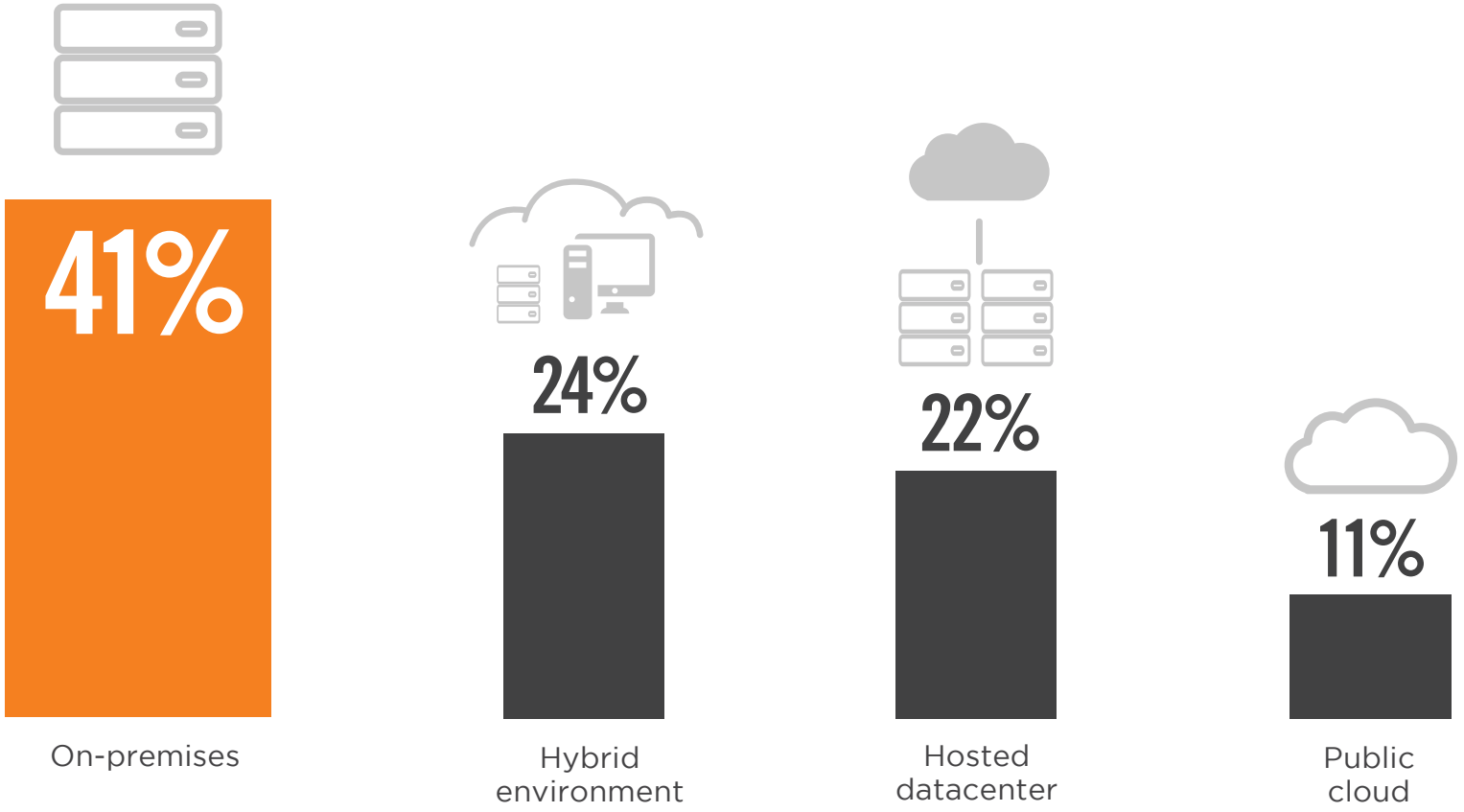
Government

Other 2%

DATA LOCATIONS

While most GDPR relevant data is stored on premises (41%), about a third of organizations (35%) store data in cloud or hybrid environments, making control over data potentially more challenging.

Where is your protected data stored?

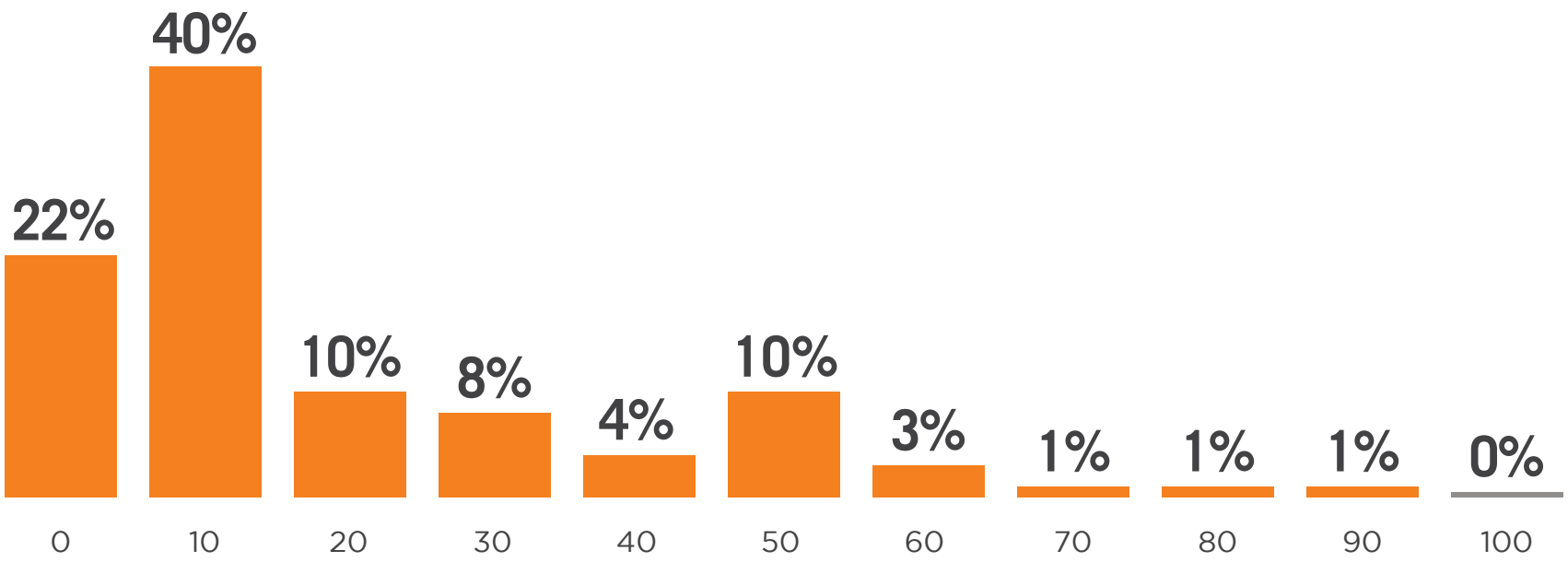


Other 2%

DATA SUBJECT ACCESS REQUESTS

60% of respondents expect to receive data subject access requests from at least 10% of their customer base.

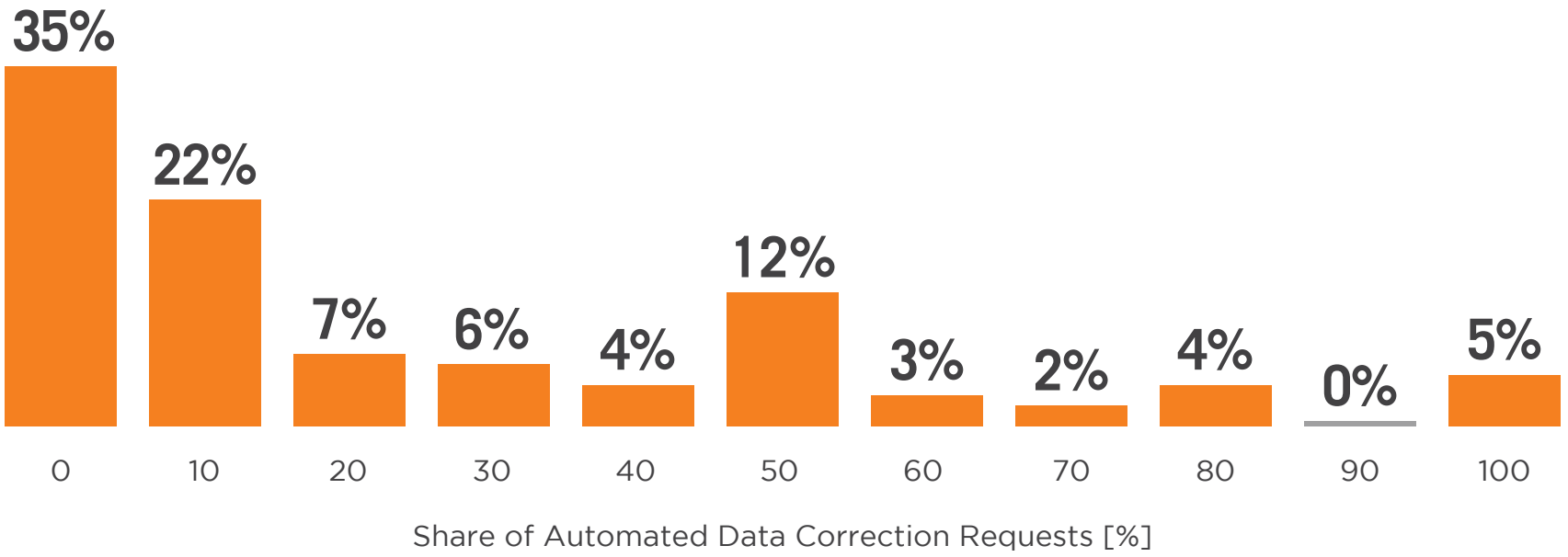
How many Data Subject Access Requests (DSARs) as a percentage of your customer base do you expect during the first year GDPR is in force?



AUTOMATING DATA CORRECTION

About a third of organizations don't believe they can automate any of the data correction requests coming from customers. Among the organizations who believe they can partially automate, the most common estimate is between 1% and 10%.

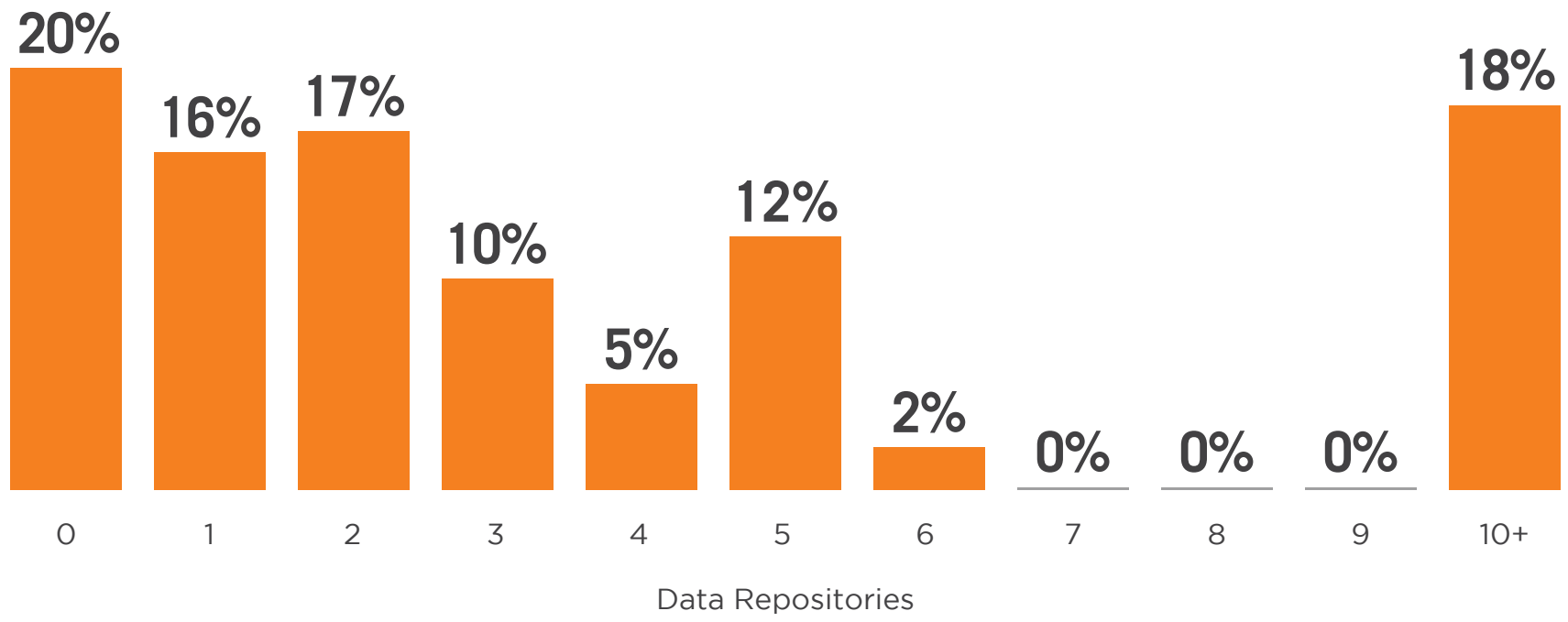
What percentage of Data Subject Corrections do you expect to automate?



AFFECTED DATA REPOSITORIES

60% of organizations in our survey have 5 or fewer data repositories subject to Data Subject searches.

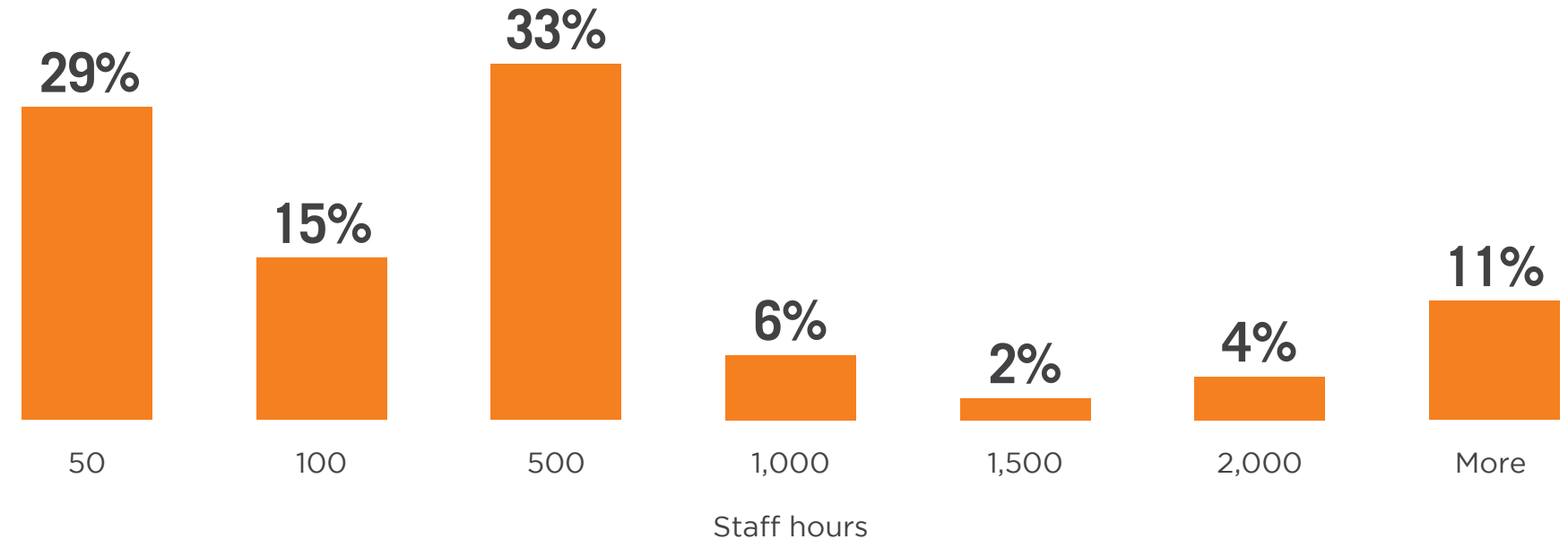
How many of your data repositories do you expect to be subject to Data Subject searches?



HOURS SPENT ON GDPR COMPLIANCE

The majority (77%) expects to spend 500 or fewer staff hours on GDPR compliance this year.

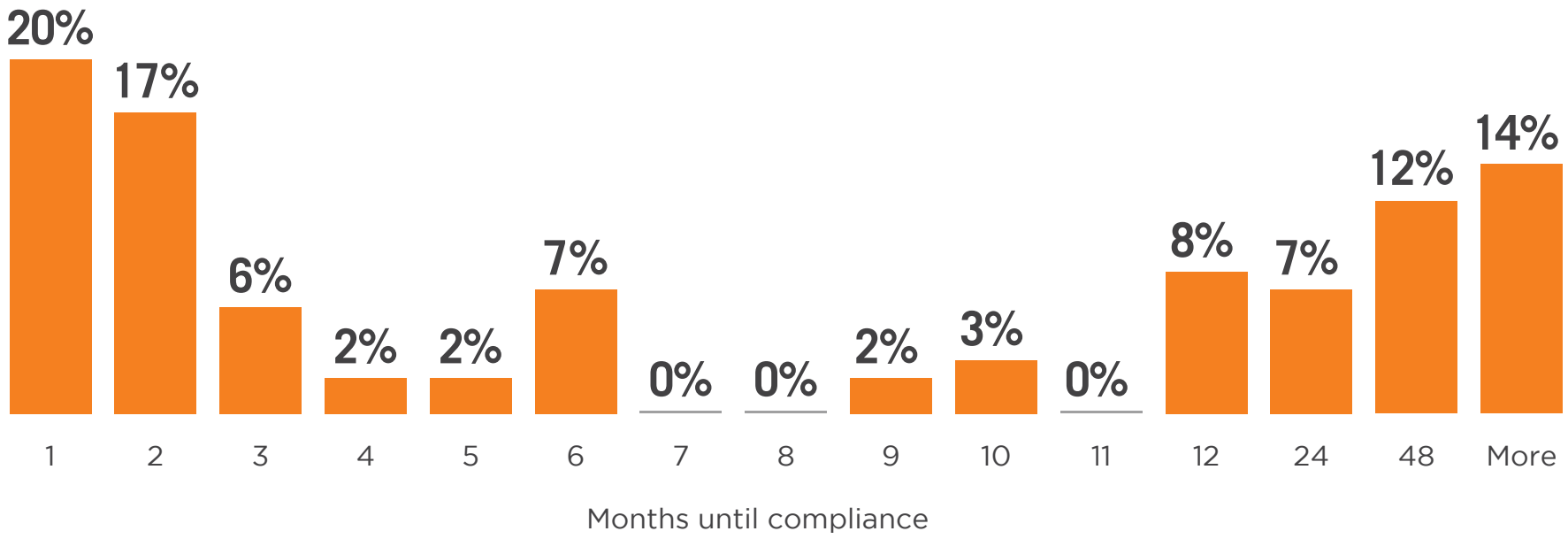
How many staff hours do you expect to spend on your GDPR compliance efforts this year?



COUNTING DOWN TO GDPR

More than a third (37%) expect they will need two months or less from the survey date to become GDPR compliant. The majority (63%), however, expects to need more than two months, with 14% expecting to need over 48 months.

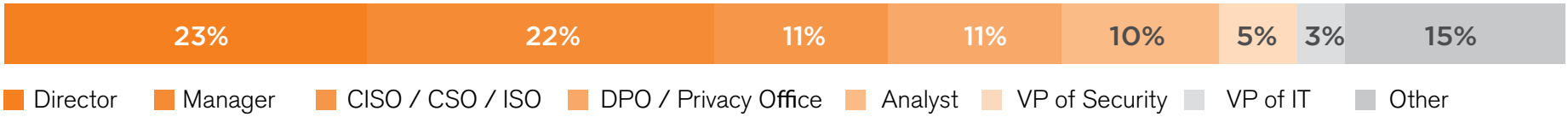
How many more months do you expect it to take for your organization to become fully GDPR compliant?



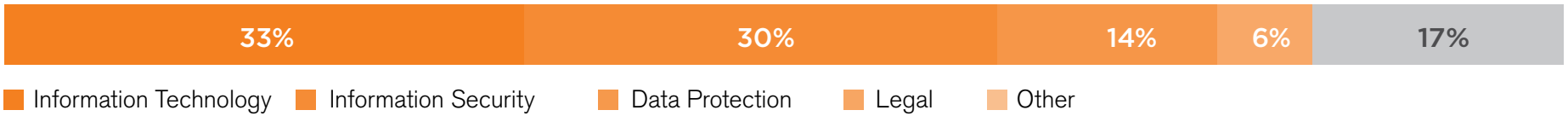
METHODOLOGY & DEMOGRAPHICS

The 2018 GDPR Compliance Report is based on the results of a comprehensive online survey of over 531 IT, cybersecurity and compliance professionals to uncover the perspectives of organizations on the impact of the new data privacy regulation, how prepared they are, and how they plan to be in compliance with the new law. The respondents reflect a representative cross section of organizations of varying sizes across different industries.

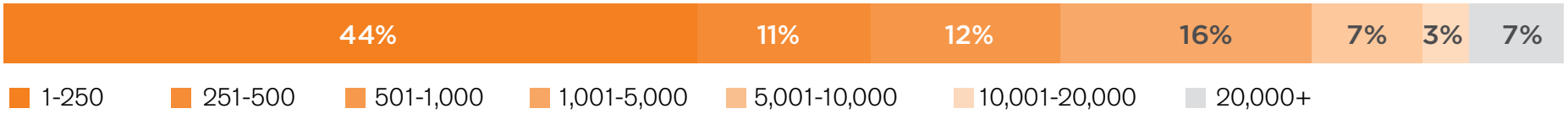
CAREER LEVEL



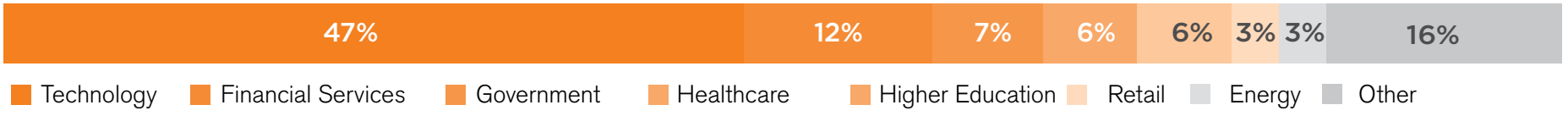
DEPARTMENT



COMPANY SIZE



INDUSTRY



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 Blog

Subscribe to our blog which provides in-depth threat intel and IT security best practices from Alert Logic experts

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

GDPR Solution Page

Most GDPR compliance requirements concern organizational measures related to processes, policy, and documentation. Unlike mandates such as PCI DSS or ISO-27001, there are no prescriptive, detailed security controls that security professionals can use for guidance. We can help!

https://www.alertlogic.com/solutions/compliance/gdpr-compliance/

On-Demand Webinar

GDPR: Ready or not, here it comes

Tune in to hear security best practices to help reduce cyber risk, as well as to identify ways to bolster what you have done so far to address the upcoming GDPR deadline.

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