EU General Data Protection Regulation

"TO BE OR NOT TO BE" COMPLIANT TO THE GDPR: "A SEA OF TROUBLES"

To be, or not to be

“To be, or not to be, that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles ...”

Peter Haase

Diploma Physicist, University of Bonn

HPE NonStop Systems Expert Programmer and IT Consultant – from 1981

Former GTUG Representative

IT Trainer for Programmers and System Manager – from 1992

Privacy Policy Manager Certificate of IHK Koblenz

Consultant for Safety Audits, Data Protection Officer and Data Privacy Consultant - from 2011

Disclaimer

I am not an expert in international law.

I do not know about all the relationships between international law and EU law.

But suppose, You want to play according to GDPR rules ...

and all companies within the EU (and outside) have to ...

EU-GDPR

REGULATION (EU) 2016/679
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

on the protection of natural persons
with regard to the processing of personal data
and on the free movement of such data,
and repealing Directive 95/46/EC (*General Data Protection Regulation*)

99 articles and 173 recitals

It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety
and directly applicable in all Member States.

Agenda

- Requirements of the GDPR
- What is to be done in a hurry?
- Status of preparation - an overview
- “Fight” or “Suffer”

GDPR - *Complete the mandatory Program in European Privacy!*

It concerns all companies, authorities and associations.

There are new guidelines for technology and organization.

Customers get more rights,
supervisory authorities judge more strictly,
fines are much higher.

There is only a very limited timeframe to prepare.

Process personal data correctly

- Documentation of all personal data processing
- Evaluation of all processes according to these principles:
  1. Lawful – fair – transparent
  2. Specified purpose
  3. Data minimisation
  4. Accuracy
  5. Storage with time limitation
  6. Integriy – Availability – Security
- Risk check of all processes
- Consultation of the supervisory authority on all processing with high risk

Obey the new rules in IT safety

IT Safety Management

- Plan / Do / Check / Act -> Plan / ...

„data protection by default“ configuration

„data protection by design“ of software

- Encryption
- Performance and scalability
- Design for data deletion and long term locking
- Desaster recovery

State of the Art: **Products from the IT marketplace**

Process new rights and obligations

- Consent of data subjects may be no longer legitimate.
- All contracts on data processing must be adjusted, and therefore negotiated anew.
- To correctly exercise the rights of the data subject - a new management procedure is needed!

Art. 5 GDPR
Principles relating to processing of personal data

Accountability

The controller

(“the natural or legal person, public authority, agency”)

shall be responsible for,

and be able to demonstrate compliance.

Status of preparation - an overview

A. The Race to GDPR: A Study of Companies in the United States & Europe

Sponsored by McDermott Will & Emery LLP - Independently conducted by Ponemon Institute LLC

Publication Date: April 2018

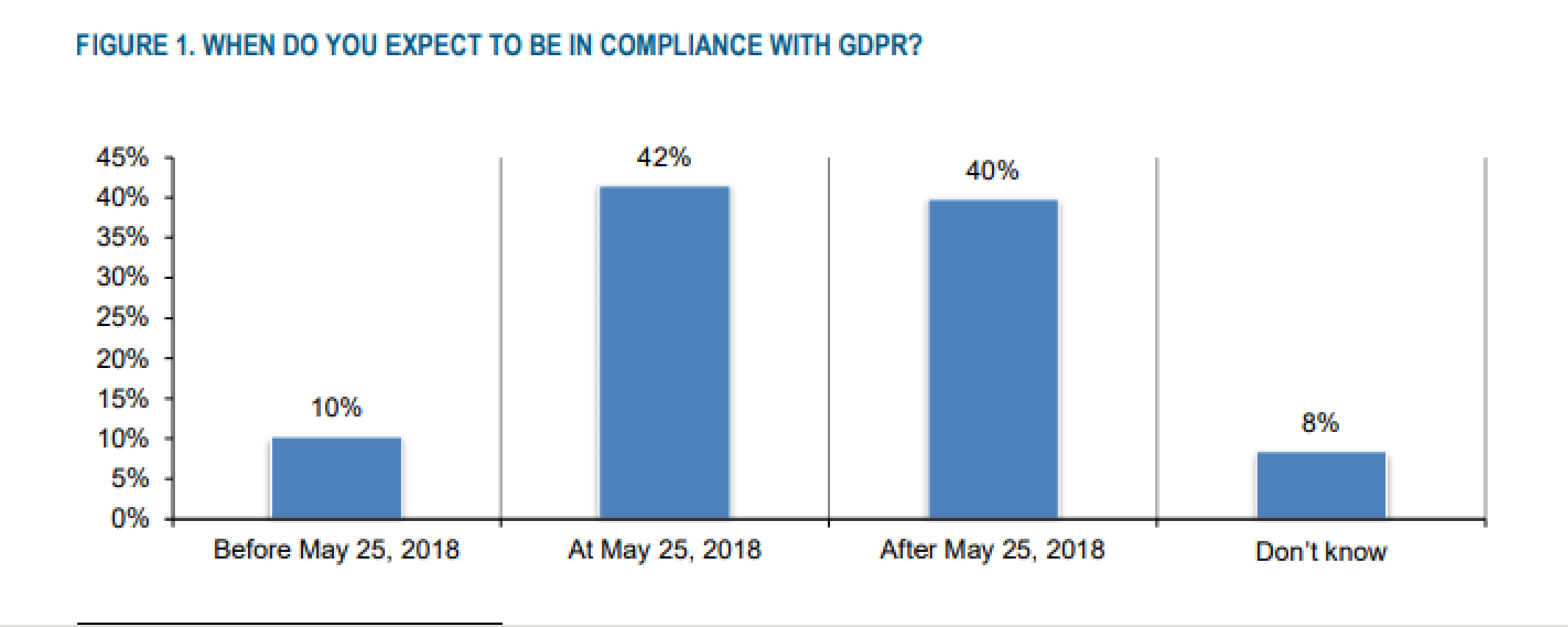
B. 2018 GDPR COMPLIANCE REPORT

Sponsored by
Alert Logic | AlienVault | Cavirin | Data443 | D3 Security | Haystax Technology | Securonix

Cybersecurity Insiders

Research done: end of 2017

A: Date of Compliance



A: Importance of Compliance

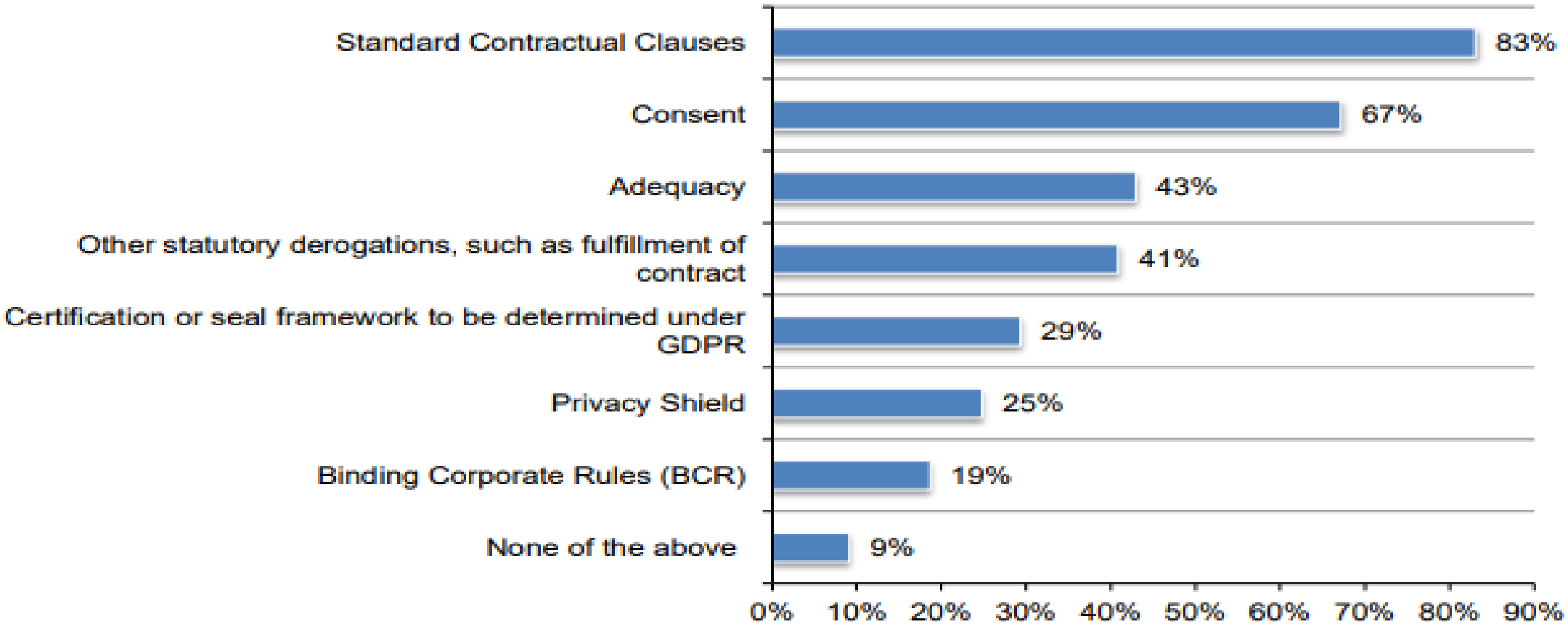
FIGURE 4. PERCEPTIONS ABOUT THE IMPORTANCE OF COMPLIANCE WITH GDPR

Strongly agree and Agree responses combined

A: Transmission outside EU

FIGURE 10. MECHANISMS USED TO TRANSMIT EU PERSONAL DATA OUTSIDE OF THE EU

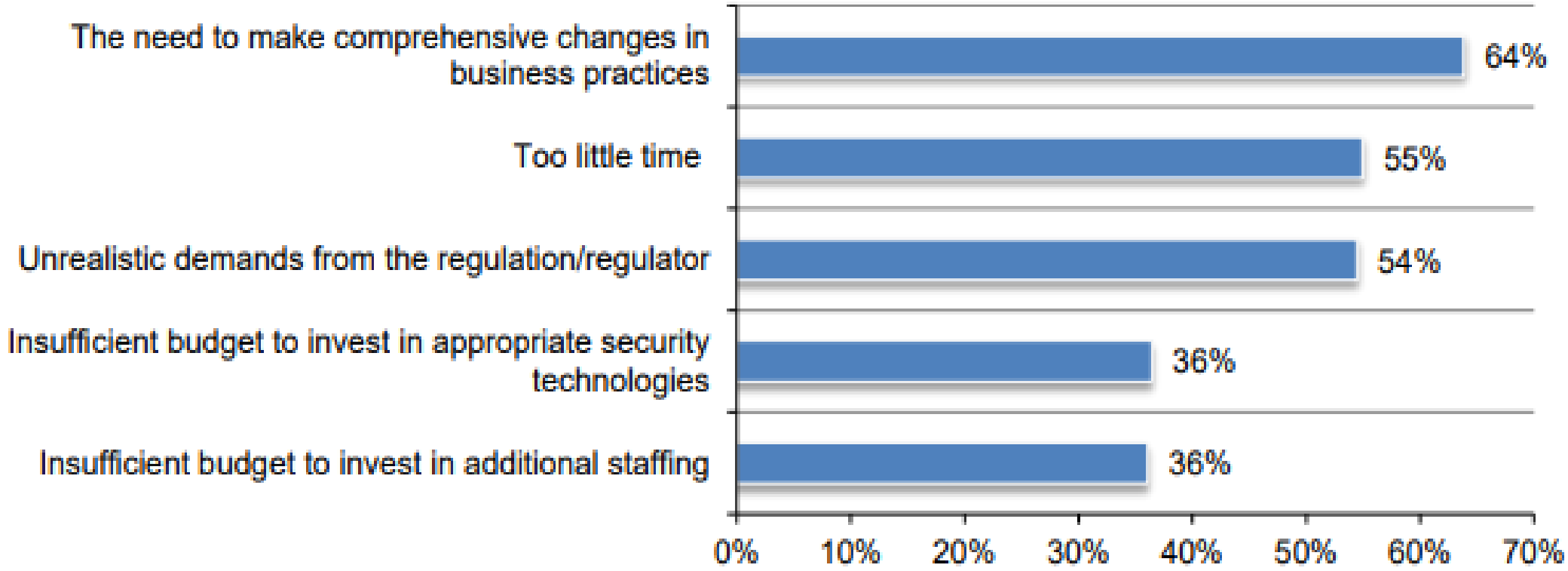
More than one response allowed



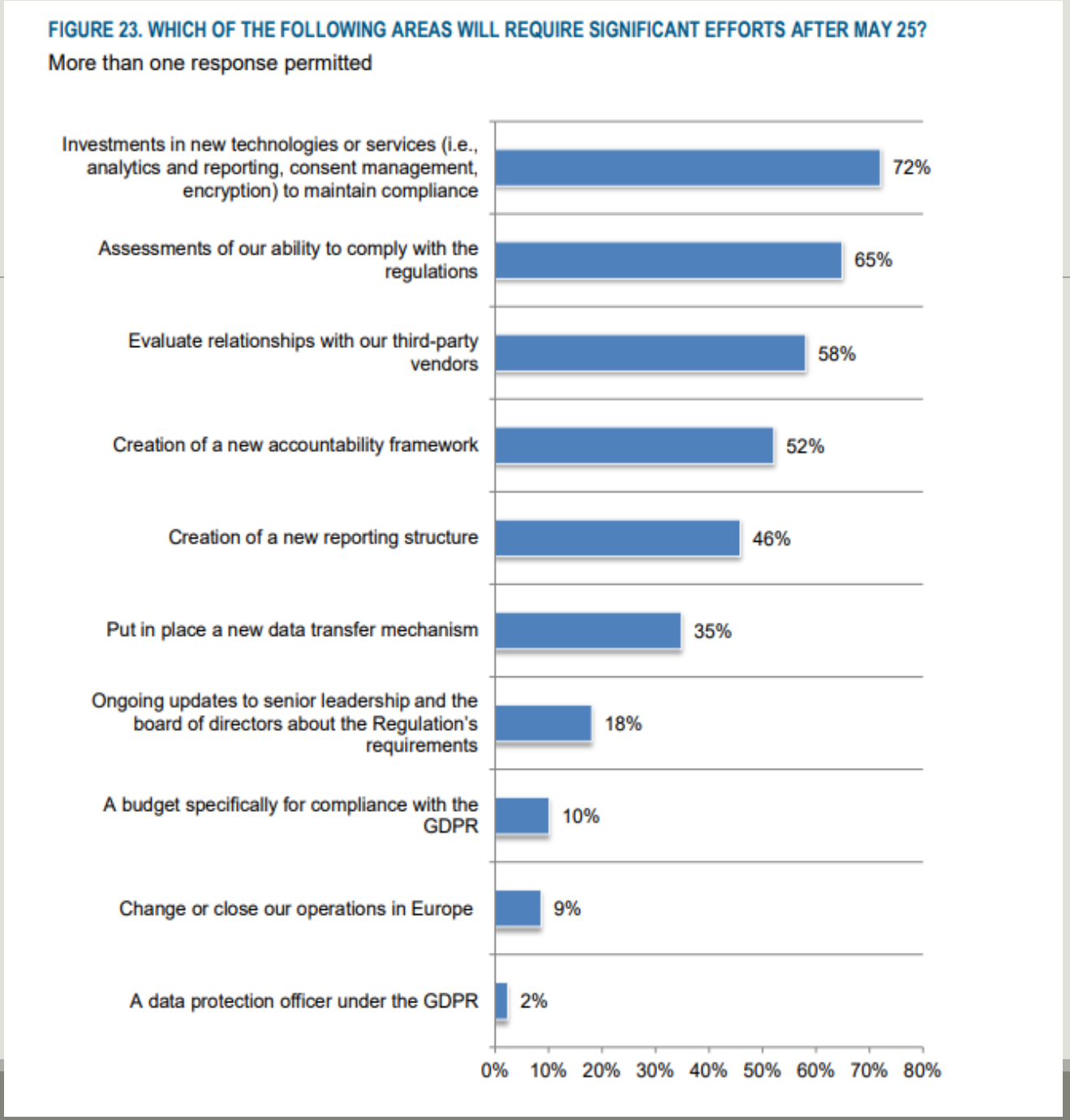
A: Barriers to GDPR Compliance

FIGURE 16. WHAT ARE THE BARRIERS TO GDPR COMPLIANCE?

Three responses allowed



A: Future Plans



B: KEY SURVEY FINDINGS – part1

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.

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.

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%).

B: KEY SURVEY FINDINGS – part2

A majority of 56% expect their organization's data governance budget to increase to deal with GDPR challenges.

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.

Find lawyers to answer these questions:

„take arms against a sea of troubles“

- **Is the EU entitled to regulate non-public sector organisations?**
- **Is the prohibition with permit reservation of the GDPR legally correct?**
- **Does the GDPR respect the presumption of innocence,**

  the prohibition of self-incrimination,

  the principle of proportionality,

  and the principle of certainty?

OR

“suffer the slings and arrows of outrageous fortune”

Peter Haase

JIT2000 GES. FÜR RISIKOANALYSEN MBH
KIRCHSTR. 12 – D-56820 MESENICH/MOSEL

INFO@JIT2000.NET

MOBILE +49-171-8442242
PHONE +49-2673-9580050
VOICE-MAIL / FAX: +49-3212-9860123