Bloor

4 questions to ask to avoid common pitfalls of GDPR compliance

Fran Howarth

Practice leader, security

About Fran Howarth

- Senior Security Analyst for Bloor Research
- Specialises in information security, with a keen interest in data security, governance and regulatory compliance.
- 20+ years in an advisory capacity as an analyst, consultant and writer.
- Regular blogger for a number of international brands and long-term contributor to security journals.

About Bill Bradley

- Leads Product Marketing for DLP
- 20 Years of Marketing & Sales Experience
  - Field Sales, Competitive Analysis, Product Marketing & Management
- Previously at Rapid7 and General Electric

Bill Bradley

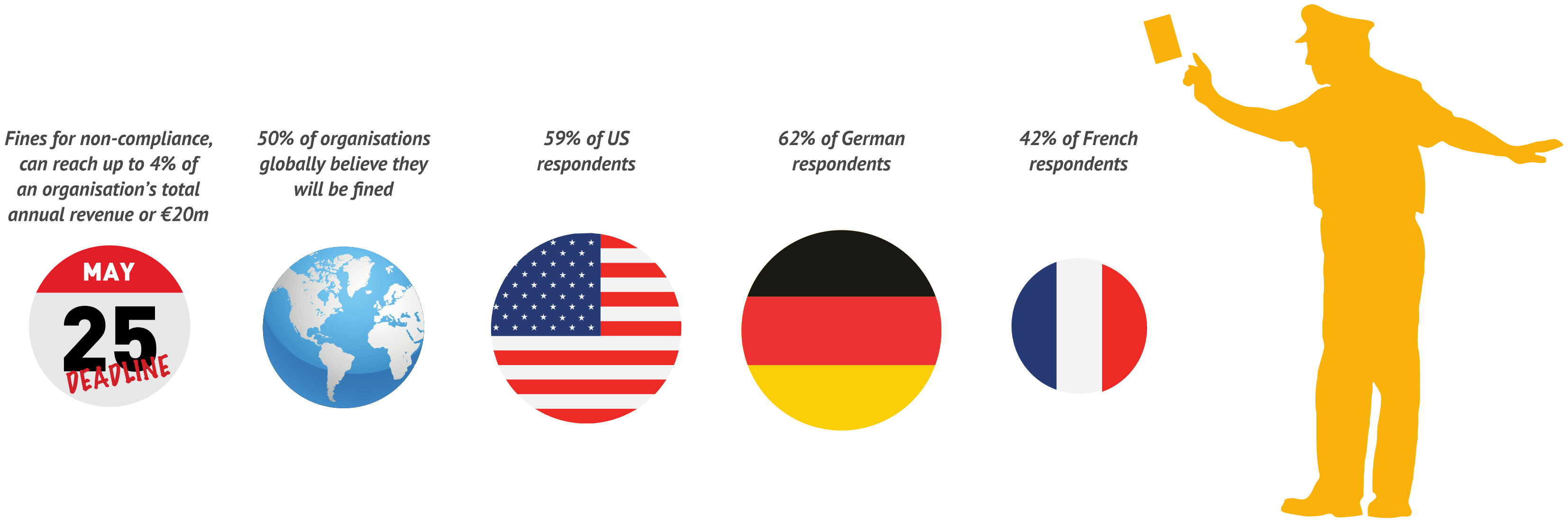
Director, Product Marketing

This time next month...

Source: www.Convert.com/GDPR

Fines for non-compliance

- Fines for non-compliance can reach up to 4% of an organisation’s total annual revenue or 20 million euros, whichever is higher.
- 50% of organisations globally believe they will be fined.
- Among individual countries, 59% of US respondents, 62% of Germans and 42% of French believe that they will be fined.



Fines for non-compliance, can reach up to 4% of an organisation’s total annual revenue or €20m

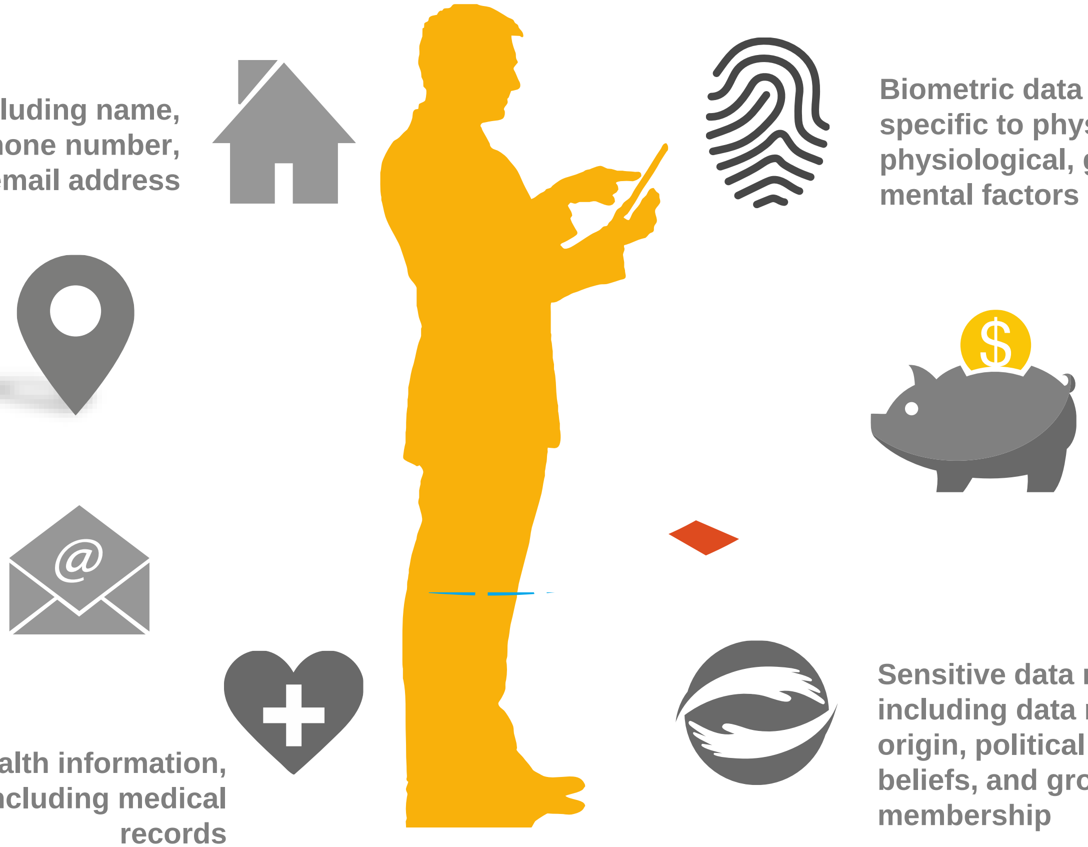
50% of organisations globally believe they will be fined

59% of US respondents

62% of German respondents

42% of French respondents

Personal data



Home and work information, including name, address, identification number, phone number, email address

Cultural information, including leisure information and hobbies, behavioural patterns and interests, location and movements

Online identifiers provided by devices, applications, tools and protocols, such as IP addresses, cookie identifiers and RFID tags

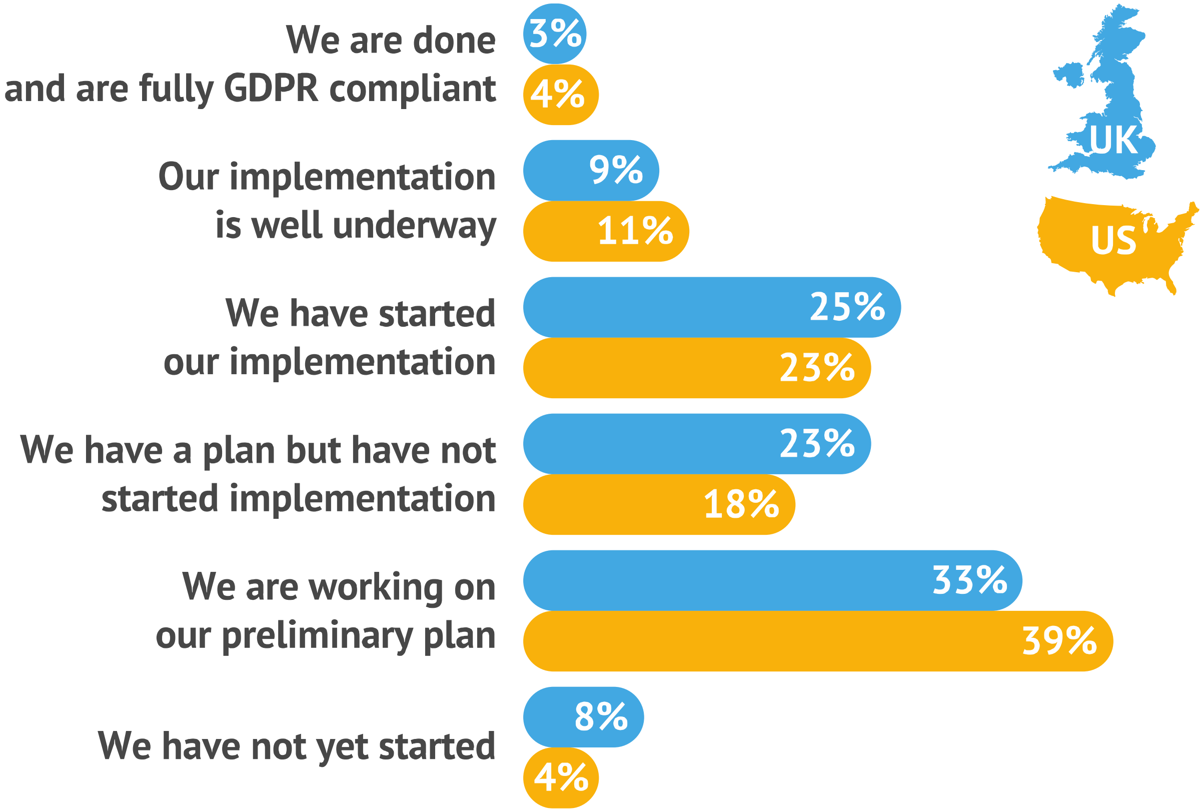
Health information, including medical records

Biometric data and identifiers specific to physical, physiological, genetic and mental factors

Financial records and other information pertinent to economic situation

Sensitive data may not be processed, including data revealing racial or ethnic origin, political opinions, religious beliefs, and group and trade union membership

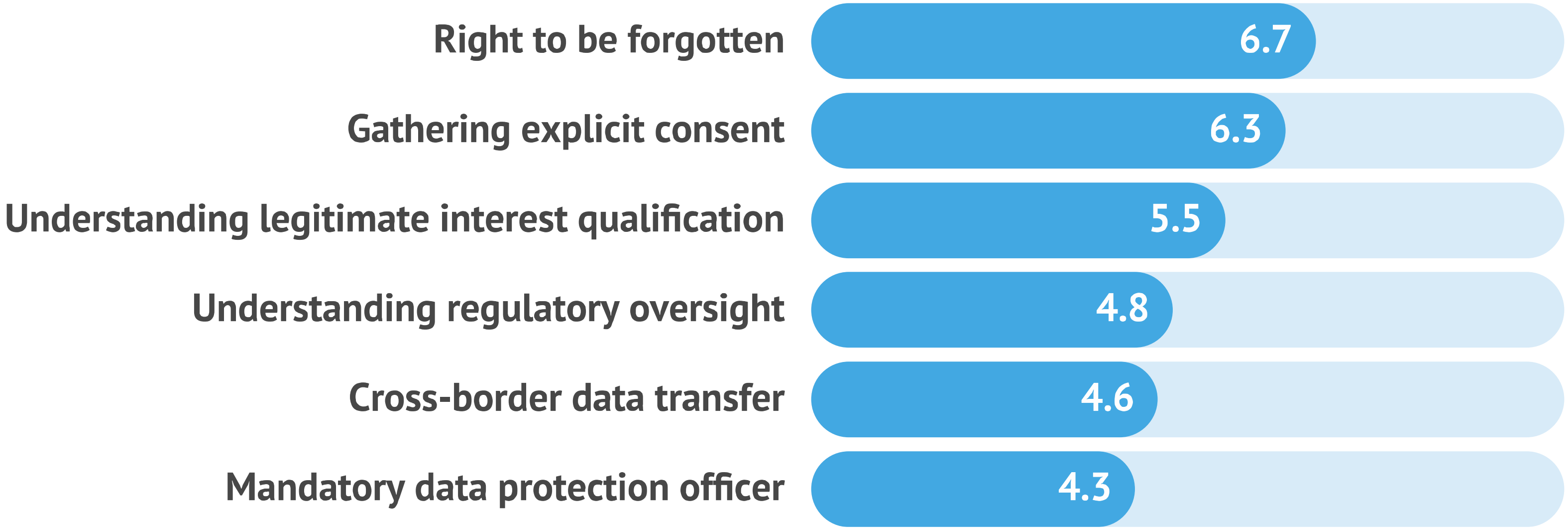
State of readiness for GDPR



Source: TrustArc

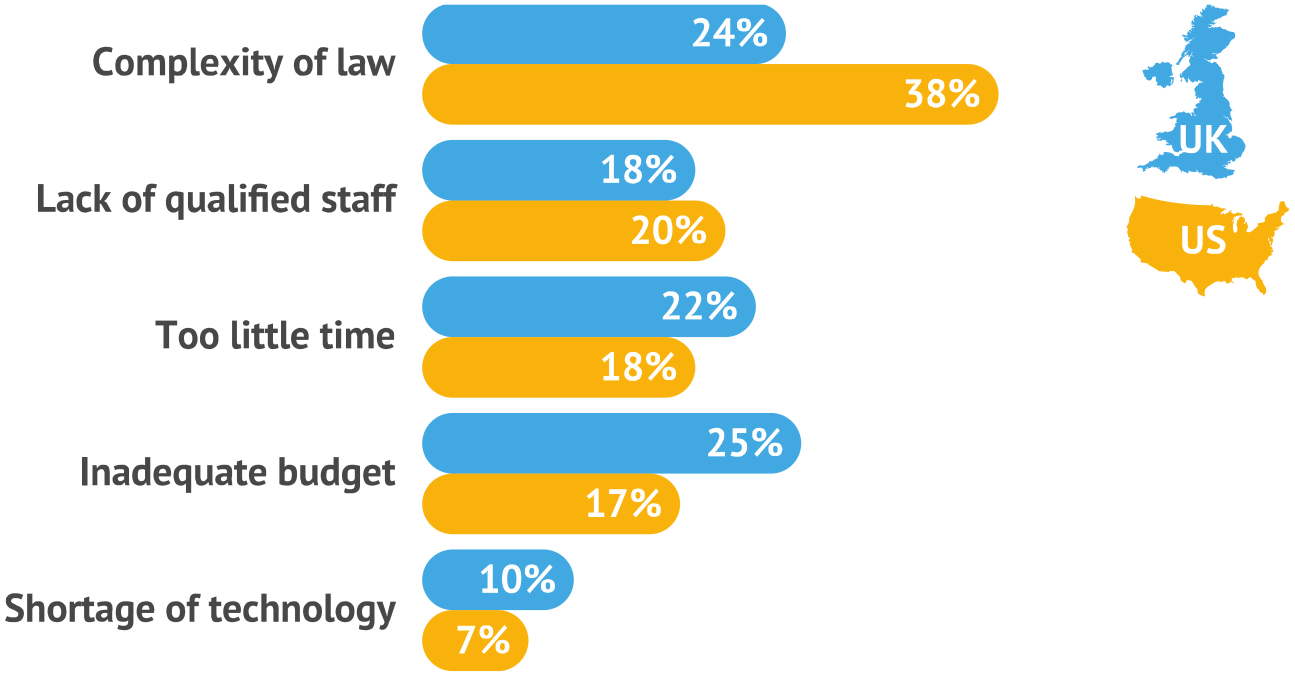
Most onerous GDPR obligations

Out of 10, where 10 is most difficult:



Source: IAPP-EY

Biggest barriers to compliance



Source: IAPP

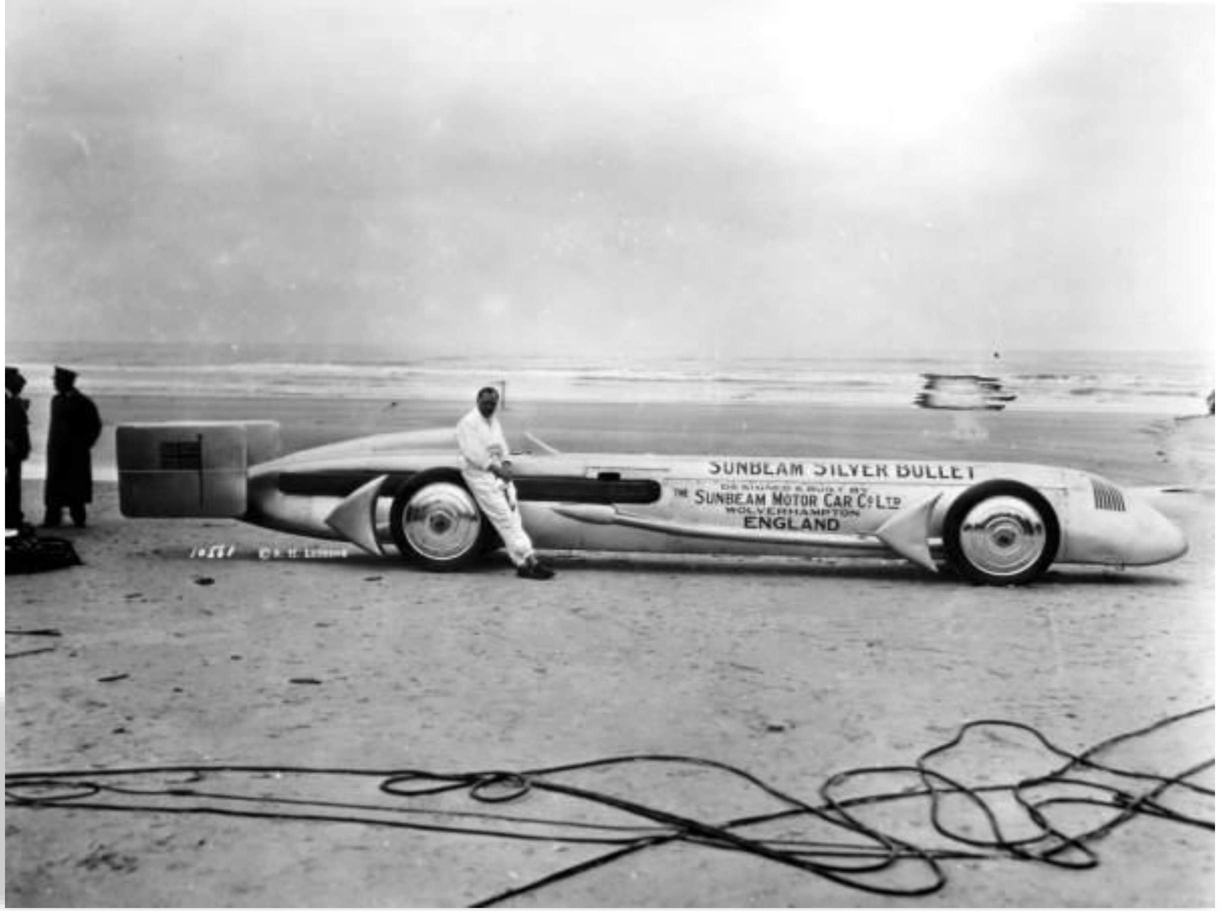
Introducing antipatterns

Photo by Socialbilitty/CC BY

The stovepipe pitfall

Photo by Chris Yunker/CC BY

The silver bullet pitfall



Source: Florida Memory Project

Putting the cart before the horse

Photo by Gary Denness/CC BY

False economy

“Our long-term plan is to find another short-term plan.”

Cartoon by Gwydion M Williams/CC BY

How to avoid pitfalls & get the GDPR programme on track

- To recap, the four pitfalls outlined describe some of the main questions you should ask yourself to ensure your GDPR programme is a success:
- **Organisational structure:** how cross-functional is your GDPR programme today? Avoid the silo or stovepipe approach. Establish a committee and get input from across the organisation.
- **Strategy:** how thoroughly have you analysed the people, process and technology needs to support compliance? Avoid the silver bullet approach. Assess your goals before buying technology or services.

How to avoid pitfalls & get the GDPR programme on track

- **Implementation:**
  What does your GDPR programme look like? Avoid the cart before the horse pitfall. Assess what personal data you have, where it is stored and how it is used before implementing compliance efforts.
- **GDPR planning:**
  How are you addressing short, medium and long term GDPR needs? Avoid the false economy pitfall. Short-term cost savings can result in higher costs over the long term.

Develop an information governance plan

- Documented information governance plan.
- Documented training programme.
- Establish data discovery plan.
- Data retention and destruction processes.
- Documented recovery procedures.

Determine what data you have

- Data discovery processes are a must.
- They must cover everything connecting to the network.
- ...and all data
- How sensitive is the data that you find?

Determine what is being done with data

- Who is accessing what?
- Create fingerprints for data.
- Monitor all network traffic.
- Enhance your access controls.

The role of DLP

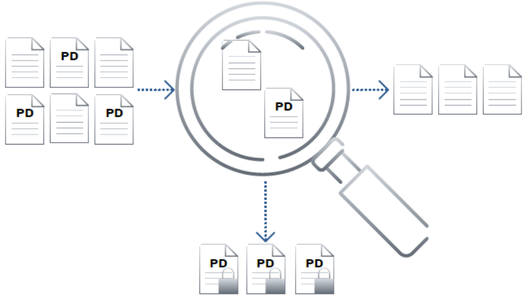
- According to the Ponemon Institute, three-quarters of organisations store sensitive or confidential corporate data in the cloud, yet this is not visible to IT in some 26% of cases.
- Gartner states that DLP has reached mainstream acceptance, with the worldwide market expected to grow from $894 million in 2016 to reach $1.3 billion in 2020.

Summary

- GDPR compliance requires an enterprise-wide approach.
- Effective data security is central to the ability to achieve compliance with the complex requirements laid out in GDPR.
- Make sure the compliance programme has a dedicated, senior executive in charge of it who can identify if it is falling into any of the pitfalls discussed today in order to pull it back onto the right path.

GDPR Success with Digital Guardian

Data Loss Prevention for GDPR



Agenda

1. People, Process, Technology for GDPR
2. DLP for GDPR
3. GDPR Assessment Offer
4. Recap
5. Q&A

People, Process, Technology for GDPR

People, Process, Technology for GDPR

People

- Data Protection Officer
- Middle Managers
- Individual Contributors
- **All Working Together**

People, Process, Technology for GDPR

People

EU GDPR

- Data Protection Officer
- Middle Managers
- Individual Contributors
- **All Working Together**

Process

EU GDPR

- Do(cument) the Right Thing
- Employees Know What to Do
- Auditors Know What you Guide Employees to Do

People, Process, Technology for GDPR

People

EU GDPR

- Data Protection Officer
- Middle Managers
- Individual Contributors
- **All Working Together**

Process

EU GDPR

- Do(cument) the Right Thing
- Employees Know What to Do
- Auditors Know What you Guide Employees to Do

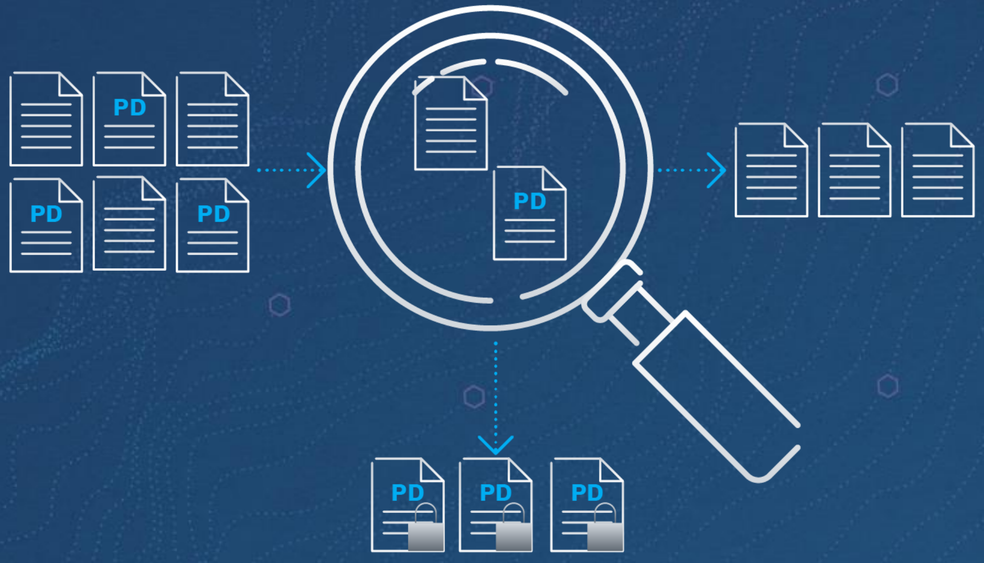
Technology

EU GDPR

- Monitor GDPR Data Flows
- Track Compliance Status
- Controls When & Where Needed

Data Loss Prevention for GDPR

- GDPR requires companies to protect personal data against breaches.

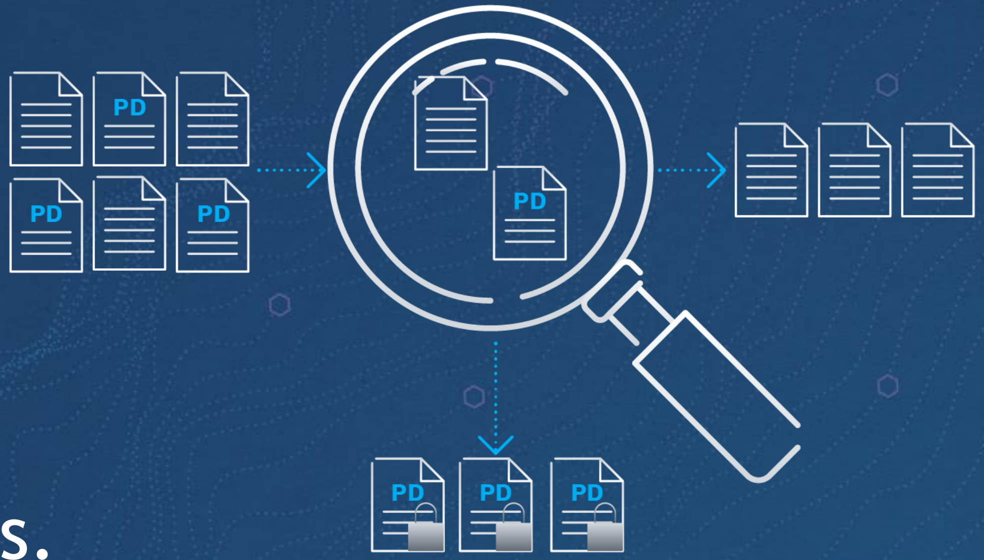


Data Loss Prevention for GDPR

- GDPR requires companies to protect personal data against breaches.

- This means measures that stop personal data from leaking

…without slowing down business processes.



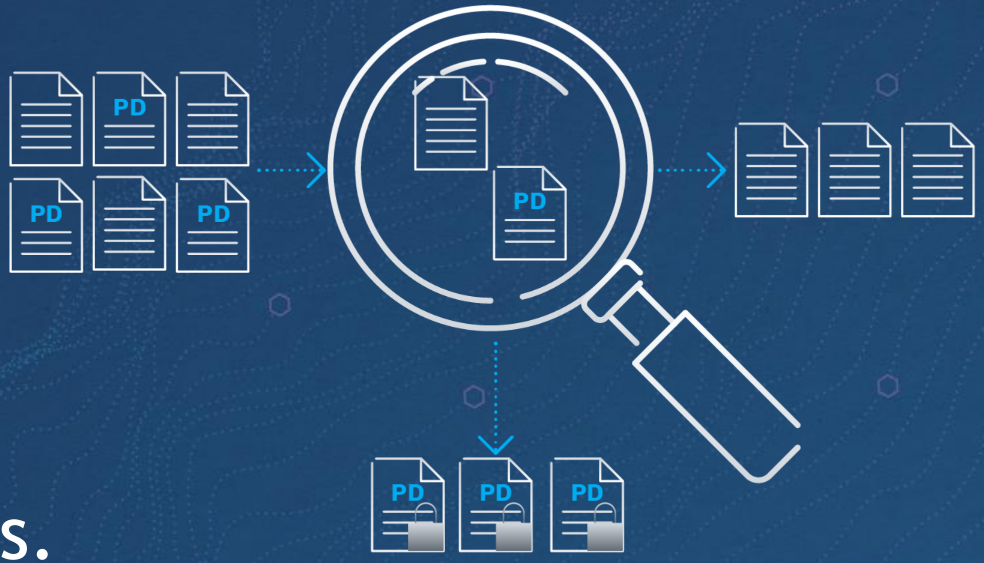
Data Loss Prevention for GDPR

- GDPR requires companies to protect personal data against breaches.

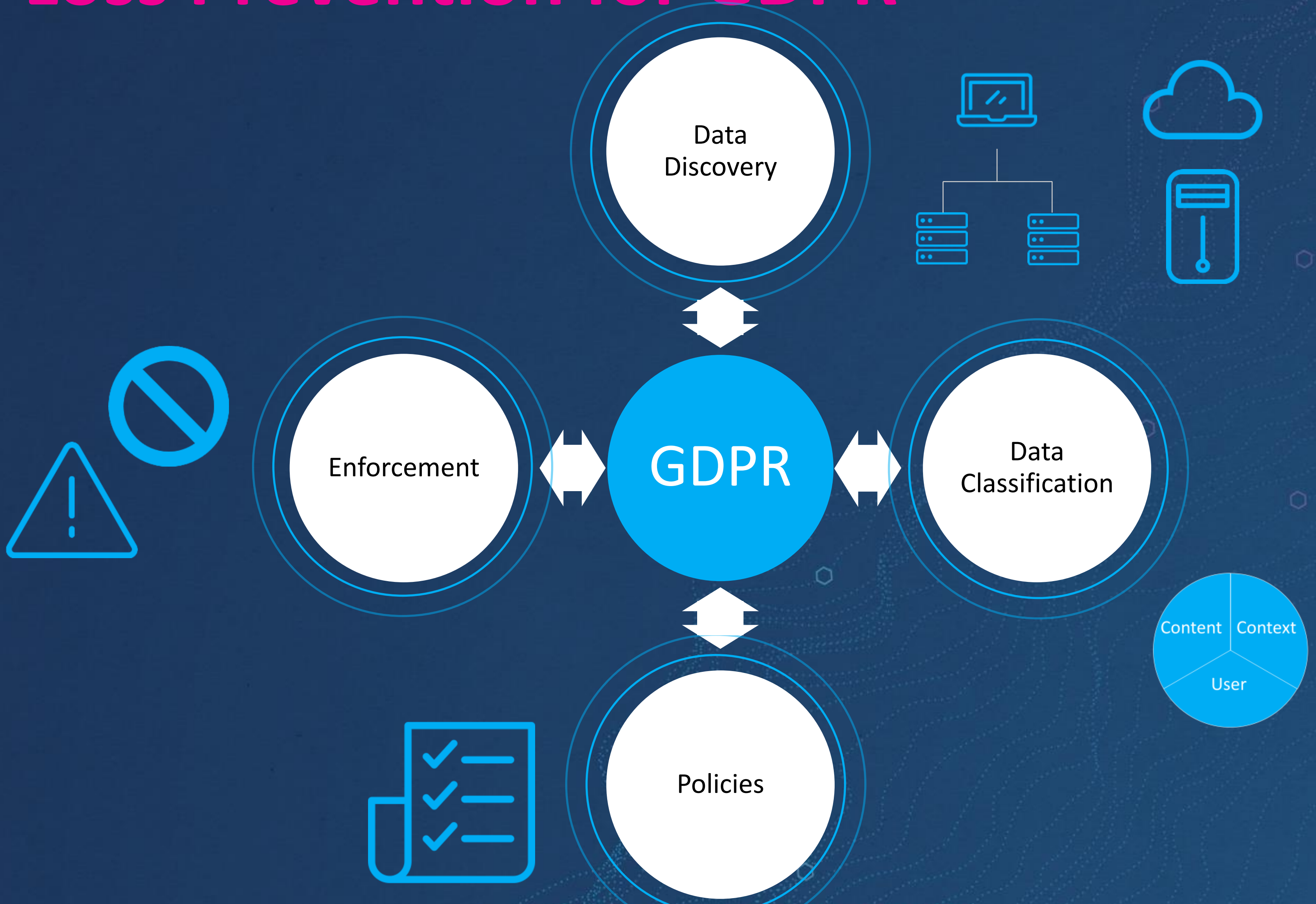
- This means measures that stop personal data from leaking

…without slowing down business processes.

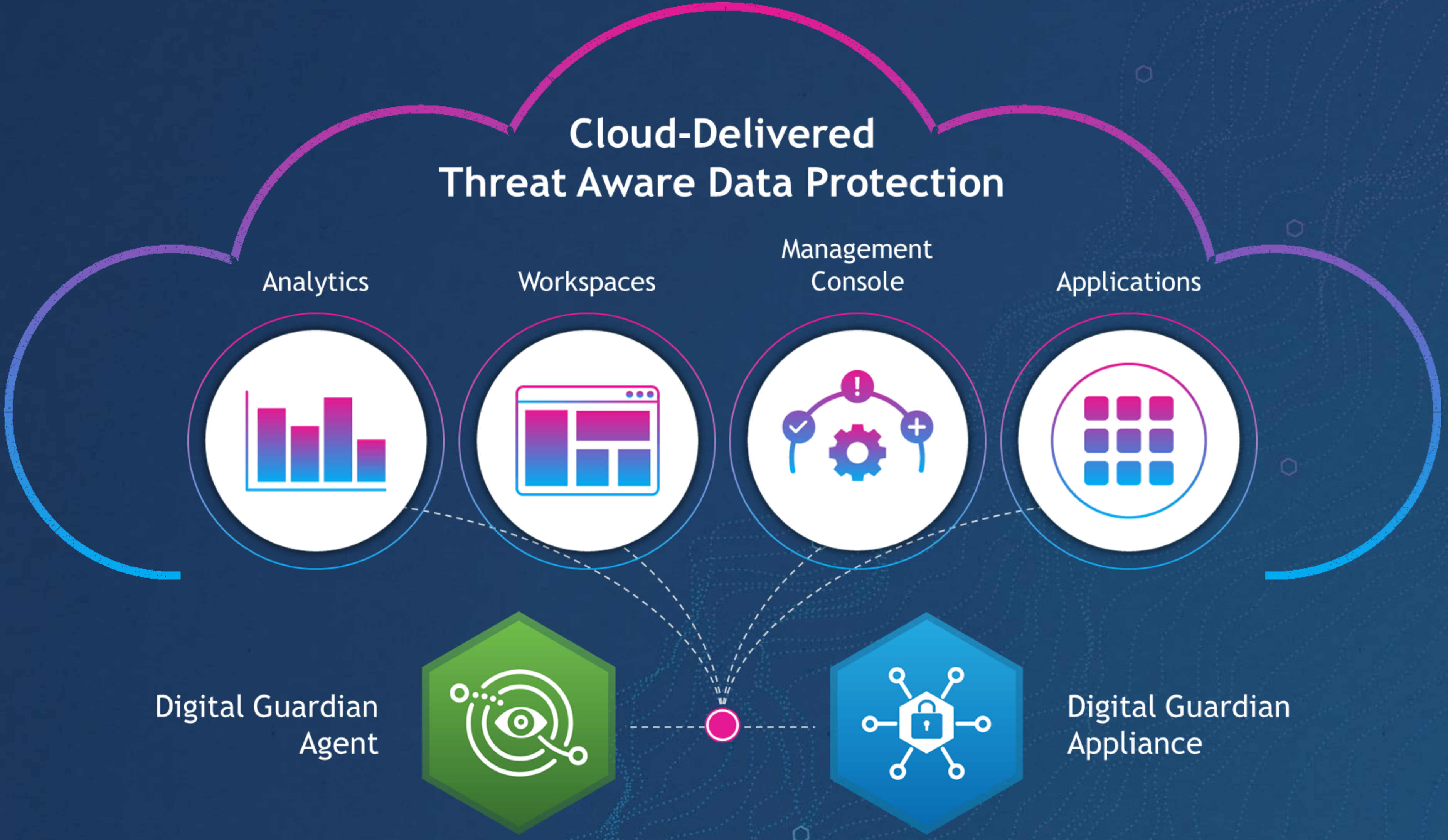
- DLP is <u>designed</u> for this.



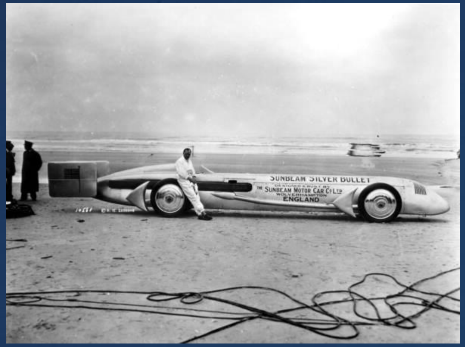
Data Loss Prevention for GDPR



Digital Guardian for Secure Compliance



Recap: The Top 4 Questions



"Our long-term plan is to find another short-term plan"

1. How cross-functional is your GDPR program today?
2. How thoroughly have you analyzed the people, process, and technology needs to support compliance?
3. What does your GDPR program plan look like?
4. How are you addressing short, medium, and long term GDPR needs?

How Prepared are You?

- Contact Digital Guardian to see if you qualify for a complementary GDPR data assessment.
- Understand:
  - Where Personal Data Resides
  - How Personal Data Flows
  - When Personal Data May Be at Risk
  - Next Steps for Your Compliance Program

- https://info.digitalguardian.com/gdpr-data-risk-assessment.html

Digital Guardian’s Next Webinar:

“Building An Efficient Data Security Program with Forrester Research”

FORRESTER®

- May 17 @ 1:00 PM ET
  - Joseph Blankenship– Senior Security Analyst- Forrester Research
  - Bill Bradley – Director Product Marketing - Digital Guardian

- Watch this webcast to learn:
  - The problems with today’s security sprawl
  - Why inefficiency is the enemy of security
  - Data protection best practices
  - How to gain efficiency in your security program