# The new (GDPR) security rules imposed by Europe and the impact on the European IT world

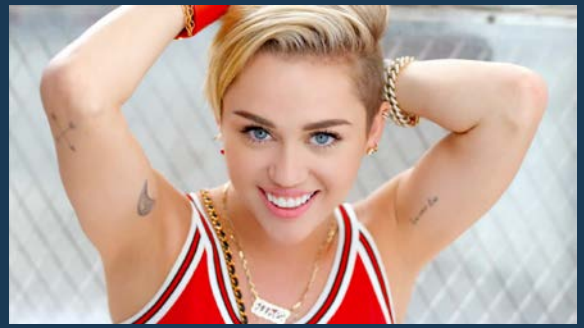
Marcel den Hartog
Senior Director, CA Technologies EMEA

ca technologies

# Who am I?

- Well, I am NOT Justin Bieber

- Unfortunately….



# I am…

- Marcel den Hartog
  - Many moons ago, started as a programmer on VSE-DL/1
  - Worked my way up to MVS (IMS and later DB2)
  - Joined Pansophic Systems in 1986 and Computer Associates in 1991
    - Pre-sales Mainframe & later Distributed as well
    - Linux Architect working for Product Development
    - Product Marketing Security
    - Now (Product) Marketing MF & Distributed
  - Studied accountancy while working

# Reform of EU data protection rules

- *The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU – and regardless of where their data is processed.*

- The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The Directive for the police and criminal justice sector protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.

- On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU. The European Parliament's Civil Liberties committee and the Permanent Representatives Committee (Coreper) of the Council then approved the agreements with very large majorities. The agreements were also welcomed by the European Council of 17-18 December as a major step forward in the implementation of the Digital Single Market Strategy.

- On 8 April 2016 the Council adopted the Regulation and the Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament.

- On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the **Regulation** will enter into force on 24 May 2016, it shall apply from **25 May 2018**. The **Directive** enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

- 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)

- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

# Emerging Themes

**TRUST**

**PROTECTING DATA**

**SECURITY**

**GLOBAL DATA FLOWS**


**ROLE OF TECHNOLOGY: IDENTITY, IAM, APIs, CLOUD, IOT**



ca technologies

# EU General Data Protection Regulation

## Scope/ Goal

- Applicable: Across European Union
- Goal: Strengthen user data protection / ease business compliance burden
- Timeline: Enters into force 2018, significant work ahead

## Why should you care?

- Range of new requirements and process changes
- Protecting data and security core to compliance
- Definition personal data
- Heavy fines of up to 20 million EUR or 4% global revenue

# GDPR

## NEW REQUIREMENTS

Data protection by design/default

Data protection impact assessments

Data protection officers (veiligheids-consulenten)

## WITH NEW RIGHTS/ SIGNS TO USERS

Certifications/seals/ codes of conduct

Data breach notification

Right to be forgotten/erasure

## TECHNOLOGY STRATEGY

Companies will need to understand where there data is, how they collect it, and who can touch it

## STRONG ROLE FOR IDENTITY

Strong, transparent, and enforceable identity policies and tools for authorization and authentication to ensure compliance

http://www.dp-institute.eu/nl/cruciale-periode-breekt-aan-voor-general-data-protection-regulation/

# GDPR - Data Security

1. Technical and organisational measures: non exhaustive list (art. 32)
2. SECURITY Breach Notification system:
   - Report to Authorities (art. 33):
     - Without undue delay, where feasible not later than **72 hours**, after having become aware of it.
     - Exception: unless unlikely to result in risk for rights and freedoms of individuals
     - Notification requirements (phases possible)
     - Document
   - Report to Data Subjects (art. 34)
     - IF likely to result in risk for rights and freedoms of individuals
     - Exceptions that can drive business opportunities (e.g. Technical and Organisational measures in place)

# Be warned.. The DPO… (apologies for not translating..)

- 2.1.1 Vlaams Besluit

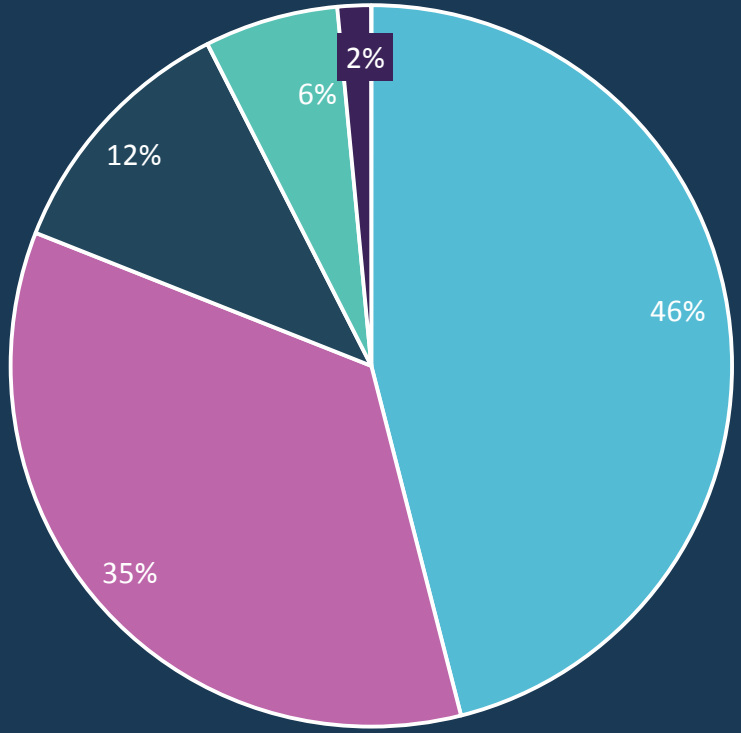
- Artikel 17 bis van de Belgische Privacywet bepaalt dat via een Koninklijk Besluit de specifieke bepalingen omtrent de aangestelde voor de gegevensbescherming worden bepaald. Dergelijk KB is echter nog niet opgesteld. De huidige rechtsgrond voor het aanstellen van een DPO is in Vlaanderen te vinden in het Besluit van de Vlaamse Regering van 15 mei 2009. Dit besluit formuleert de verplichting om een DPO aan te wijzen voor (1) iedere instantie die een authentieke gegevensbron beheert die persoonsgegevens bevat, (2) iedere instantie die elektronische persoonsgegevens ontvangt of uitwisselt, en (3) iedere entiteit die overeenkomstig artikel 4, §3, van het decreet van 18 juli 2008 aangewezen is door de Vlaamse Regering en persoonsgegevens verwerkt.

- Met behulp van gepaste technische en organisatorische maatregelen beschermt de DPO persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens

- A DPO CAN be an employee, but also a third party

# Awareness of the GDPR

During the week that the GDPR was announced, only 46% reported being fully aware of it…

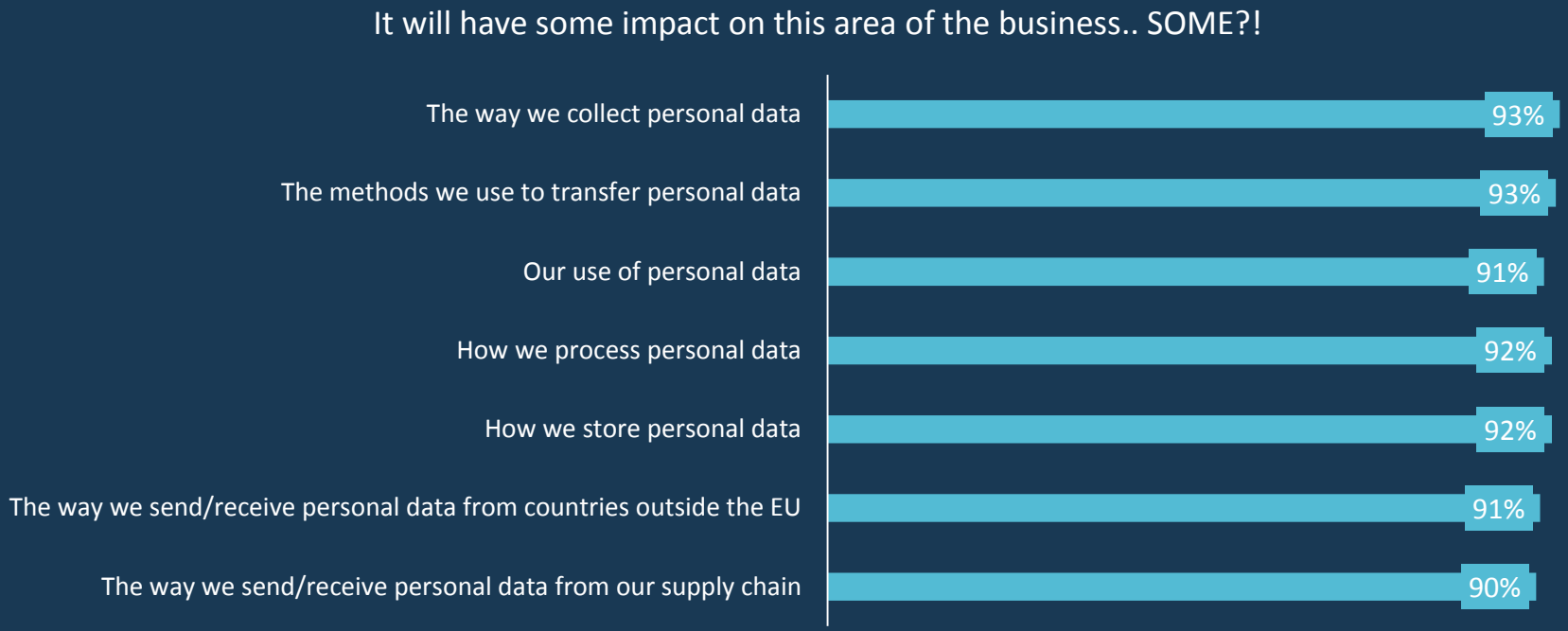





ca technologies

# Impact of the GDPR on the business

## Many areas of respondents' businesses will be affected by the GDPR

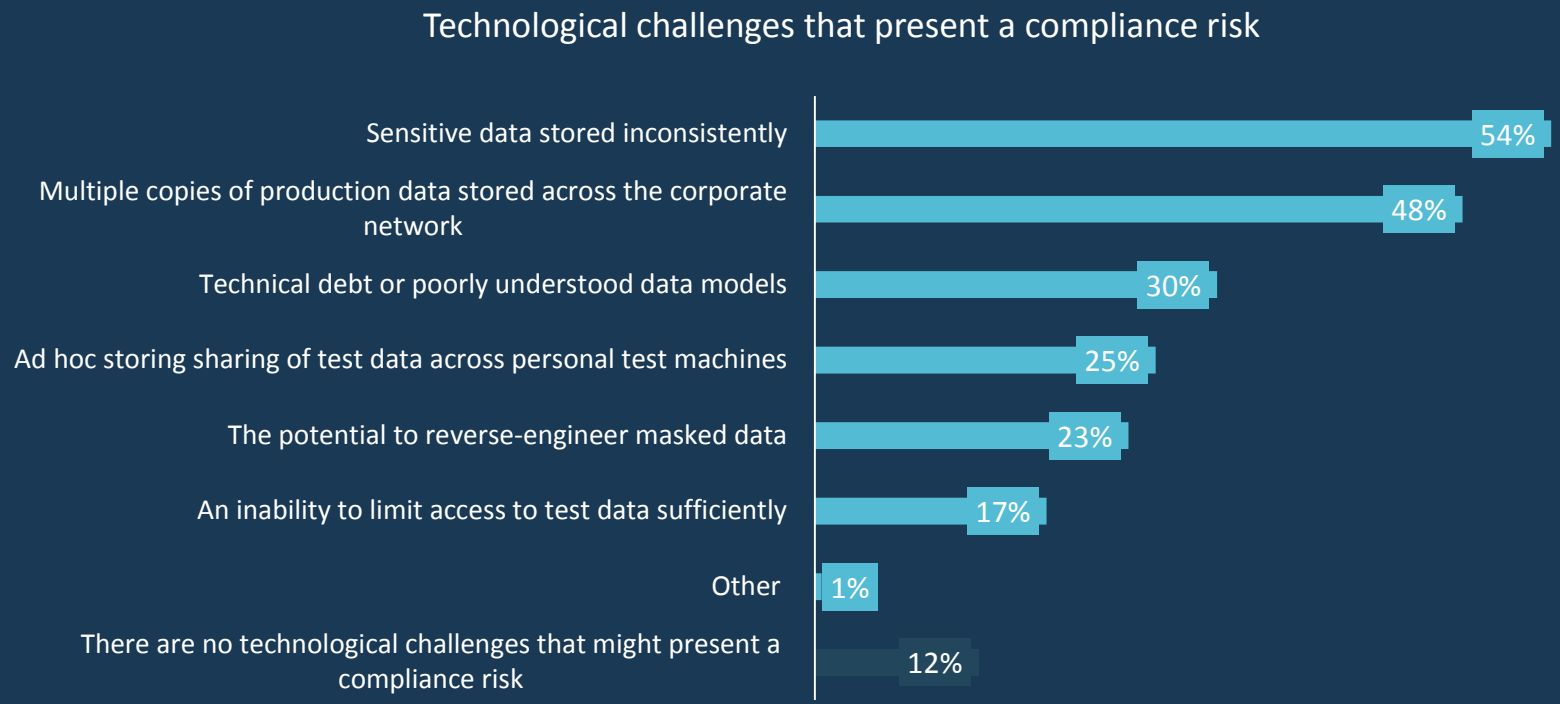





ca technologies

# Technological challenges in GDPR compliance

## Over half report that sensitive data is stored inconsistently within their organization



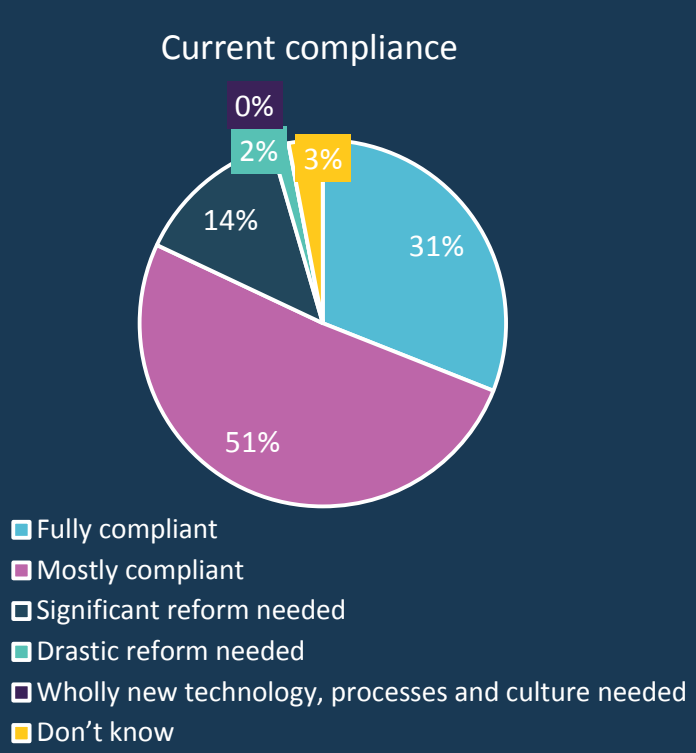

I started to highlight the ones where I thought…. OF COURSE!! But I stopped…

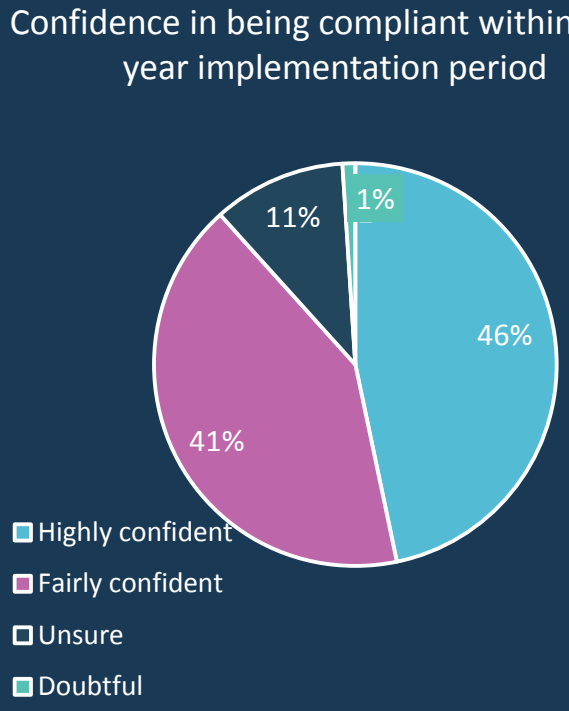


ca technologies

# Current testing practices are not up to scratch…

…and under half are highly confident that they will be compliant within the implementation period



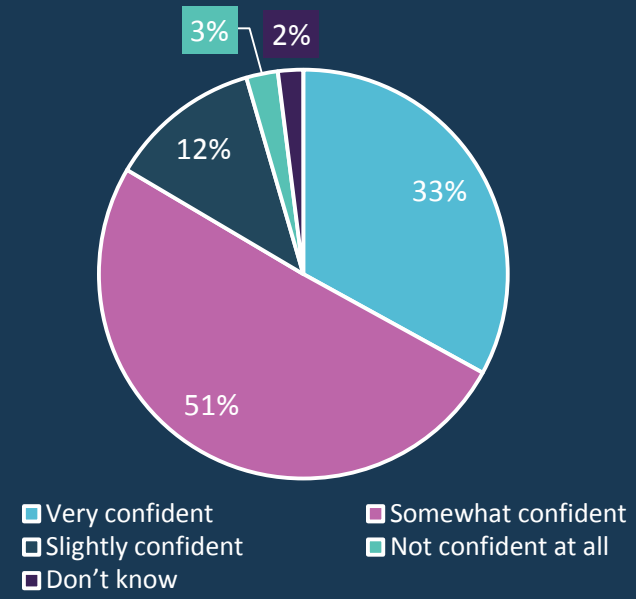



ca technologies

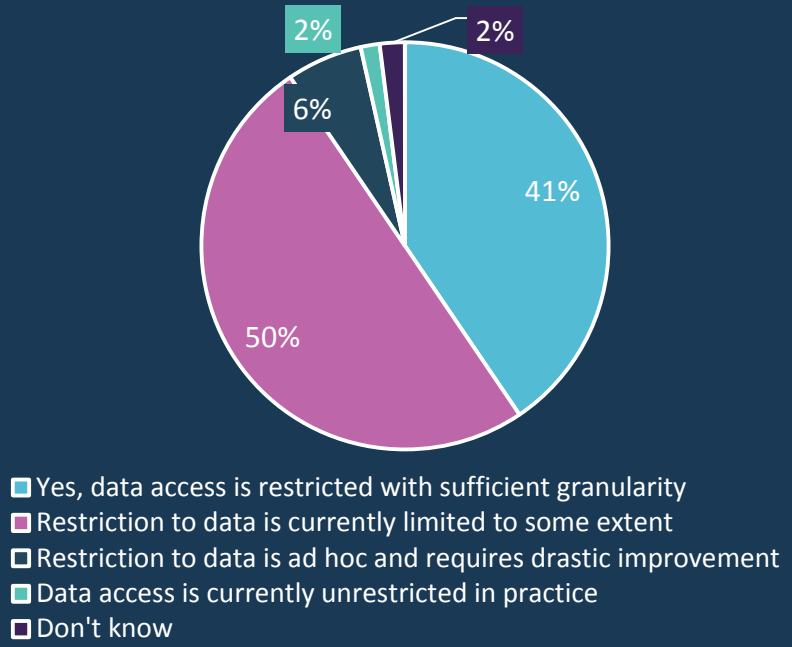
# Compliance gaps in current processes

## The processes in the majority of surveyed organizations are not compliant with the GDPR

Confidence in prompt identification of every piece of content



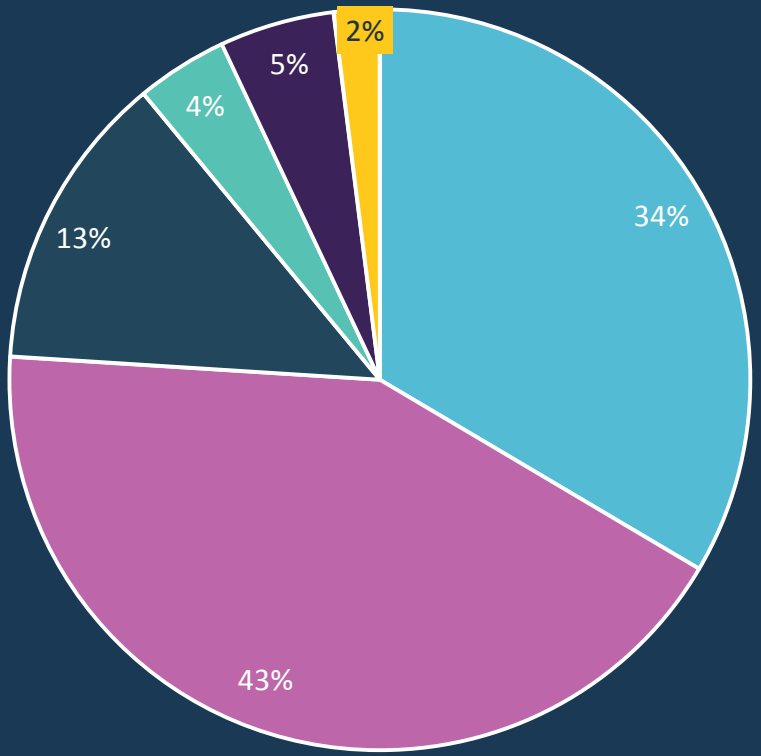

Confidence in limiting data access (in line with the GDPR)





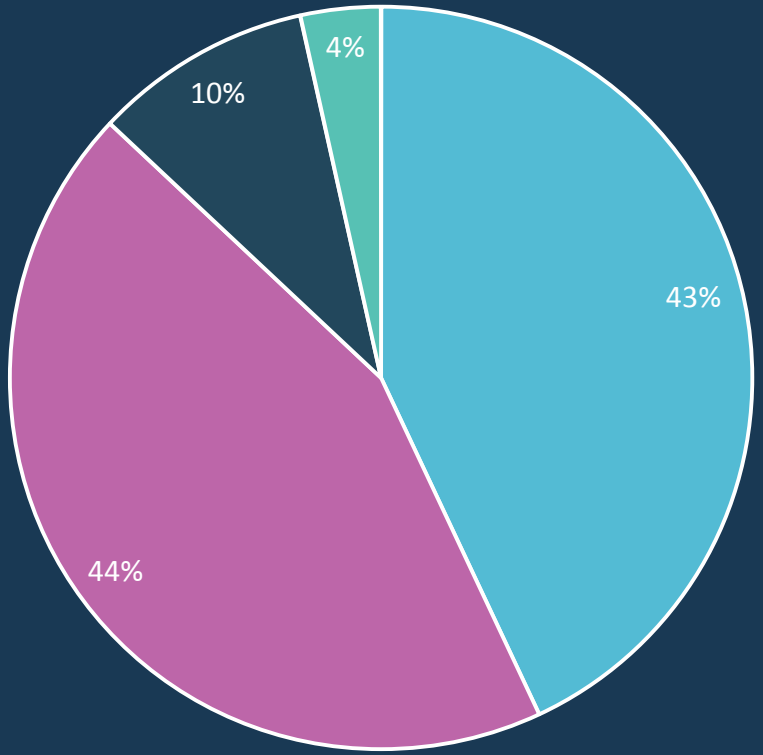

ca technologies

# Erasing customer data “without delay”




- Completely confident
- Somewhat confident we could do it quickly enough, but not convinced we would catch every piece of data
- Somewhat confident that we could do it – but it wouldn’t be quickly enough
- Somewhat confident it might be possible - but need to gather more info
- Not confident at all
- Don’t know

# Allowing customers access to their data




- Yes, fully
- Yes, but only in one or two formats
- No, we don't have any way to do this
- Don't know, need to check with my team



ca technologies

# The challenge for testing

1. You need to know that testers have consent to use the data they're using
2. You therefore need to know exactly where sensitive data is, but data models are poorly understood and testers share and store data in an ad hoc manner
3. Understanding the specific repercussions of the GDPR for current test data management practices such as data masking

# What does it mean to “Pseudonymize” data

- To mask data so that it can be processed in testing in a way “compatible” with the purpose for which consent was given
- Under the GDPR, this does not require that data is wholly “anonymous”, but that it is not “directly identifying”:
  - All “direct identifiers” must be removed so that the data subject could only be identified using external information
  - Mechanisms and organizational measures must be in place to keep the additional information separate

# But when we are done with this, we are done!!

Right?

Wrong….

# More Regulatory Activity

| | |
|---|---|
| **EU GENERAL DATA PROTECTION REGULATION** | ▪ Strengthen protection of data<br>▪ Reduce administrative burdens |
| **EU NIS DIRECTIVE** | ▪ Increase cyber readiness for both government and industry |
| **US CYBER THREAT INFO SHARING** | ▪ Enhance real-time sharing of cyber threat data<br>▪ Automate data transformation and PII removal |
| **PAYMENT SERVICES DIRECTIVE 2 (PSD-2)** | ▪ Drive safer, more innovative payment systems across EU |
| **US-EU PRIVACY SHIELD** | ▪ New (model?) framework for data transfers |

# EU Network and Information Security (NIS) Directive

APPLICABLE ACROSS EU

**BUT** EU Member States may implement differently—risks fragmentation

GOAL IS TO ENHANCE CYBER READINESS IN GOVERNMENT AND BUSINESS

Critical infrastructure and "essential" service providers

TIMELINE

Entry into force in first half 2018

- New security requirements like security breach notification system

- Incentives to invest in security technologies to strengthen protection.
- New tools to automate management and reporting.

- Even if you are not in scope, per se, requirements will flow down to suppliers and partners.



ca technologies

# NIS—Who is in Scope? Who else will be affected?

## Operators of Essential Services—Critical Infrastructure

- Energy (electricity, oil, gas)
- Transport
- Banking
- Financial market infrastructures
- Health (healthcare settings, including hospitals and private clinics)
- Drinking water and distribution
- Digital infrastructure (internet exchange points, DNS service providers, top-level domain name registries)

## Digital Service Providers (DSPs)

- Online search engines
- Online marketplaces
- Cloud computing services

# US-EU Privacy Shield

**International Data Transfers in EU Context**

**ECJ and Aftermath**

**Status**

**Invalid as of Oct 6. Must review current processes.**
**Uncertainty and doubt…**



ca technologies

# When in doubt…

- Talk to your legal council
- Speak with your vendors
  - Some things have been taken care of already
- Read stuff
  - http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

# Thank you!


**Marcel den Hartog**
Senior Director
zMarcel@ca.com

@cainc

slideshare.net/Cainc

linkedin.com/company/ca-technologies

**ca.com**