CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

The impact of GDPR on Third-Party and M&A security

Dr Marco Ermini, CISA, CISM, CISSP, ITILv3, GCIH, RCSS, PhD
Senior Security and Compliance Officer, Orange Business Services

Take away

- Describe the impact of GDPR on three different but connected business processes:
  - Mergers & Acquisitions (M&A)
  - Third-party security
  - Outsourcing security

- Approaching an external organization is going to be different after GDPR is in force

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

What is this all about?

- GDPR impact has been mostly focused on technology
- Understand the general impact of GDPR on M&A prospects
- Impact of GDPR on third-party and outsourcing security
- Identify specific GDPR programs, which affect third-party, outsourcing and M&A processes
- What "privacy" means in the context of M&A activities, outsourcing and third-party

Let’s get started!

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Setting the stage

Compressed GDPR

or

“GDPR for dummies”

Three Dimensions of GDPR

- **Legal.** The GDPR is a law. **This research note is not intended as legal advice or comprehensive guidance.**
- **Procedural.** (New) roles, responsibilities, accountabilities and processes to be implemented
- **Technical.** The GDPR includes many data protection principles and requirements that must be enabled by technology, or that require technology to limit impact to internal operations

Personal Data and Privacy

- The GDPR is about protection of personal data and privacy
- Securing personal data is only a subset of all requirements
- “Personal data" in the GDPR depends on context
- Ask the company's legal advisor

Why GDPR is a concern

1. GDPR is enacted law, not an elective standard; penalties for noncompliance are potentially severe
2. GDPR is "extra-territorial“, which means it applies to all organizations that offer goods and services into EU markets
3. Reputational damage, loss of employees and erosion of customer trust are inevitable if you disregard the rights of data subjects or fail to report and deal with a breach of their personal data correctly
4. GDPR refers to the inclusion of a data processor in your business process, which broadens the attack surface for vulnerabilities and the controller's responsibility to keep informed on the data processor’s status

Implementing a GDPR program

Gap Analysis

and/or

Implement
Basic Aspects

GDPR in a Nutshell – 1/2

1. Governance and Accountability
2. Privacy “by design” and “by default”
3. Privacy Impact Assessment
4. Enforcement
5. New rights for Data Subjects (DS)
6. New obligations for Data Processors (DP)
7. Privacy Notices

GDPR in a Nutshell – 2/2

6. User consent
7. Data Protection Officers (DPO)
8. Notification of security breaches
9. Enforcement scope
10. European Data Protection Board
11. Concepts of “pseudonomysed” data and privacy seal (“EuroPriSe")

Image credits: https://www.peerlyst.com/posts/gdpr-getting-to-the-lawful-basis-for-processing-david-froud

Data Subjects rights

- The GDPR does provide data subjects with a set of rights over the administration and use of their personal data
- Organizations that control personal-data processing activities throughout the data life cycle should have less trouble enabling these rights
- The right to data portability could be assured by implementing a self-service portal; the same online platform can be used to provide transparency and notification
- The right "not to be subject to a decision based solely on automated processing, including profiling" implies a strong focus on automation of analytics and the use of the subsequent results

Data Subject consent

- It should be freely given, there can be no coercion or pressure
  - Consider employee relations

- "Consent" in the GDPR requires several conditions:
  - "*By a clear affirmative act*"
  - "*Specific*“
  - *"(As an) informed and unambiguous indication of the data subject's agreement to the processing of personal data*“

- The burden of proof that consent was obtained lies with the data controller

Recap: DC vs DP

Data Controller	Data Processor
Controls what personal data is processed	Uses data only as instructed by Data Controller
Responsible for the processing purpose (e.g. determines why that personal data is processed)	Processes data as instructed by the Data Controller
Responsible for the means of processing by the Data Processor	Must respect the contractual agreement with the Data Controller
May create third-party agreements with Data Processors and sub-Processors	May create sub-Processor agreements as authorised by the Data Controller

Data Processor = Third-Party

DC vs DP

- Organizations should be aware that they can occupy both roles in different processing activities
- Using a cloud-hosting provider's services, an organization may be a data controller and the hosting provider the data processor as it stores and processes the data on behalf of the data controller.
- Conversely, when deploying EU-based employees, the cloud provider may be the controller for the HR activities.
- Similarly, a marketing agency may be a B2B client's data processor in the initial service provision, but when it uses the data gained in contracts to enrich profiles for a campaign of its own, it is the data controller for the latter activity.

Implementing a GDPR program

GDPR Implementation Basics

GDPR Personal Data Lifecycle

Collect + Classify

- Define the purposes of collection
- Collect only the personal data necessary
- Inform data subjects
- Identify the categories and sensitivity of personal data

Process

- Process personal data lawfully, fairly and transparently
- Facilitate the exercise of Data Subject rights

Delete

- Do not keep personal data for longer than it is necessary
- Upon lawful request, erase a data subject's personal data without undue delay
- Notify any processors of the erasure request

Secure

Implement technical and organizational measures to ensure a level of security appropriate to the risk based on the nature, scope, context and purposes of processing.

Share

- Only share personal data with processors that provide sufficient guarantees
- Perform GDPR compliant cross-border data transfers

Document

Maintain records of all processing activities covering the entire personal data lifecycle

GDPR Gap Analysis How-To

- Performing a risk assessment
  - data processing activities
  - each technical and organizational control
- Developing a prioritized remediation roadmap
- Implementing technical, organizational, policy, and process improvements
- Documenting the overall control environment
  - strengths
  - weaknesses
  - intended future state

Basics of GDPR Implementation

1. Write a Privacy Notice and publish it
2. Inventory of processes and activities
3. Implement Data Retention
4. Implement Data Subject access rights and consent requests
   - B2C
   - HR
   - Procurement
5. Perform Data Protection Impact Assessment
6. Implement Security & Privacy by design / privacy by default
7. Handle personal data transfer & Third-Party management
8. Ensure Data Breach management process is in place

Art. 30, “Records of Processing Activities” – 1/2

- Art. 30 is the foundation for all compliance activities
- Opportunity to leverage information being collected to enable “flags” which indicates high-risk business processes
- Use art. 30 to set up a system which is starting to document what is collected and from who is collected
- Automate time consuming and timely processes (sending reminders, etc.)
- Setup thresholds to identify where something triggers a Data Protection Impact Assessment (DPIA) – or not
- Use this system to check cross-border data transfer points

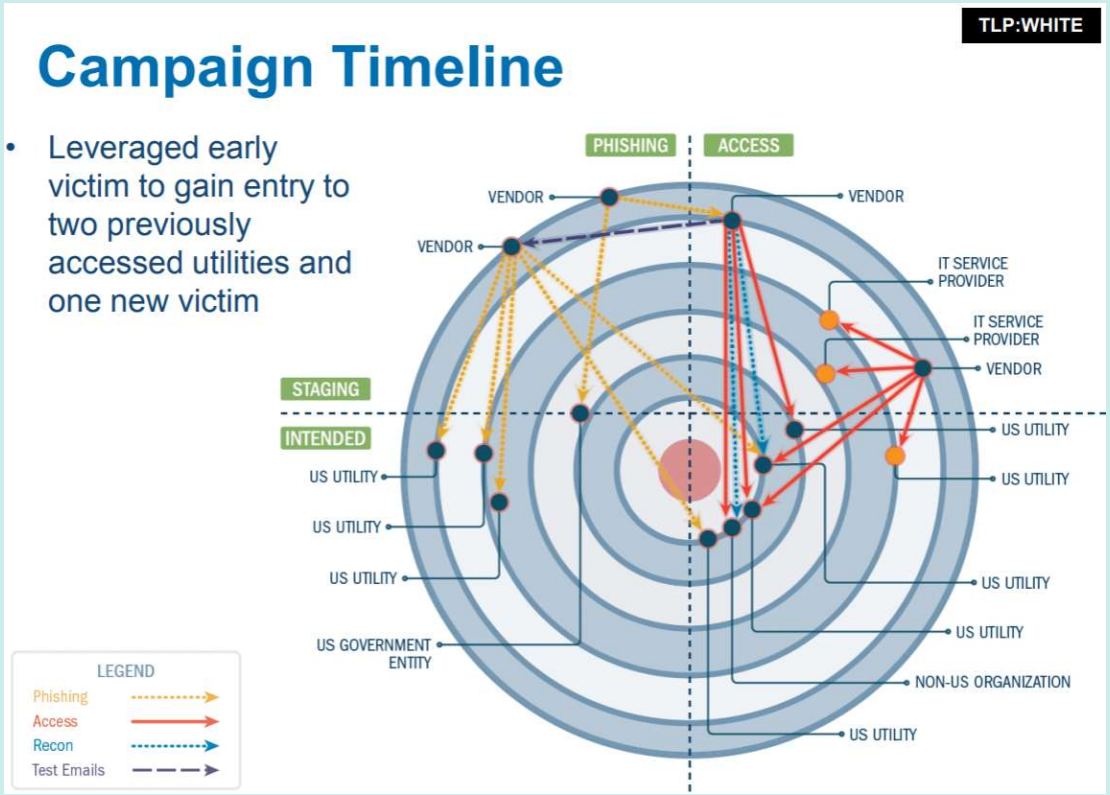
Art. 30, “Records of Processing Activities” – 2/2

- Justify the collection of data, data retention, and identify where the right consent is given – legitimate business activity?
- Setup reminder of when data needs to be “retired”
- Build-in reporting for external vendors – interactive technology, trigger questionnaires, etc.
- Make it simple for the Data Subject
  - single point of contact and front-end process (self-service portal)
  - standard templates (informative and standard)
  - backend processes codified and standardised
- Interaction as a positive experience, reflect the company positively

Information is the new gold

- Information is an asset
  - Like software and hardware assets, build an inventory
- Information is fluid
  - Include data flow diagrams
- Answer these questions & document the answers
  - What data do we have?
  - How and why do we collect it?
  - What do we do with it?
  - Where do we store it?
  - How do we secure it?
  - Who do we share it with?
  - How long do we retain it?
  - What do we do with it at end of life?

Third-Party vs Critical Infrastructure



Source: [Awareness Briefings on Russian Government Activity against Critical Infrastructure]

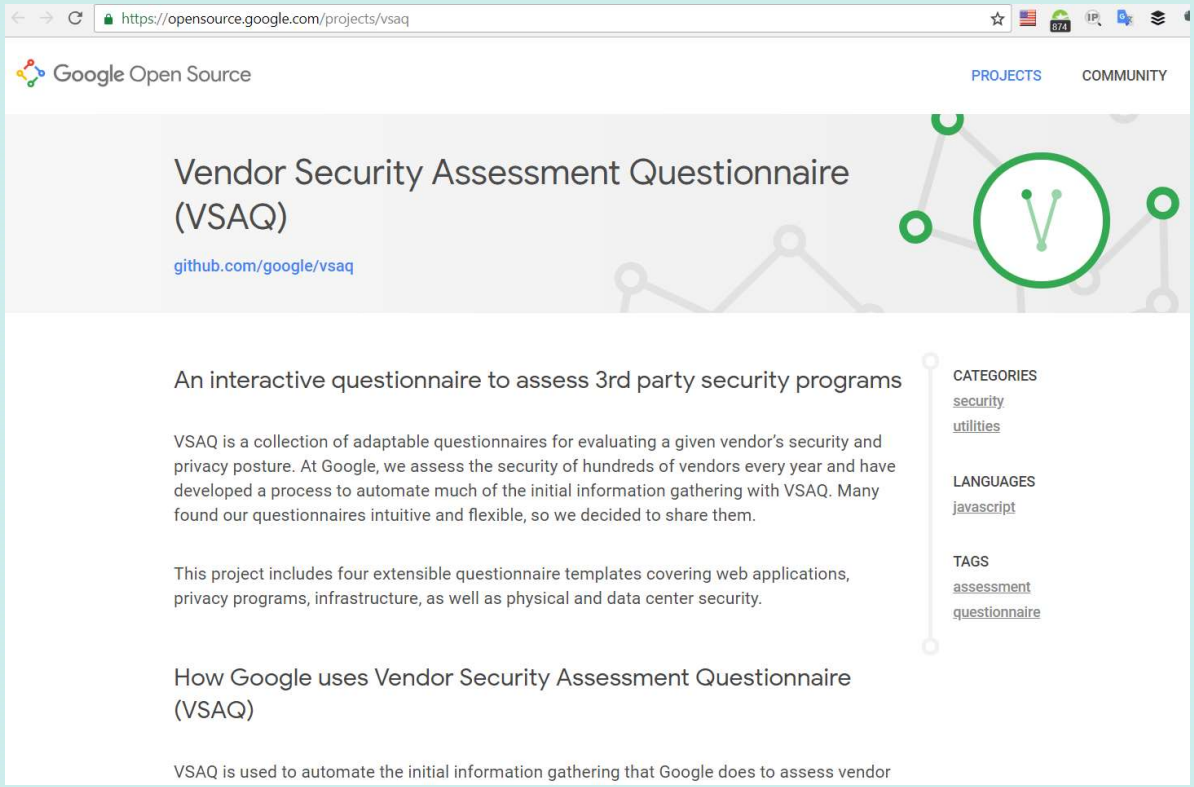
Lessons learned

- Attackers are patient (instances of laying in wait for over a year)
- Attackers know not to walk in the digital front door, preferring to hit weak vendors
- Pivoting is not confined to just a company, pivoting across companies is very real
- “Secure” vendors are not as secure as they want us to think
- When vendors brag about having certain companies as clients, they open themselves up as targets
- External firms are being used as staging and exfiltration points
- Moving between traditional IT and ICS/SCADA is relatively simple today

Third-party and GDPR

- Many organizations outsource processing of personal data with third-party service providers
  - Very little control over data, increased risk of noncompliance
  - Security posture is rarely an evaluation criterion
- Recommendations
  - Specify vendor-selection criteria
  - Add requirements as exclusion/inclusion criterion in procurement
  - Ensure adherence to the requirements throughout the lifetime of the contract by leveraging one or more assurance methods as described

Google's VSAQ

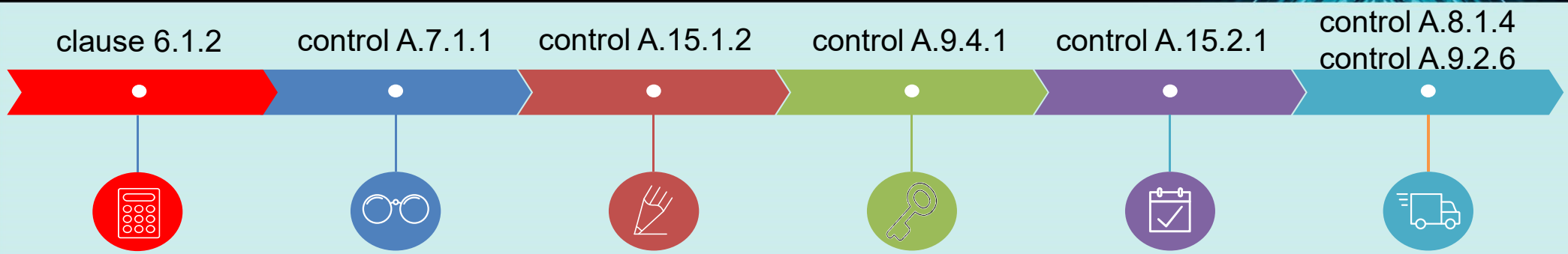


Source: Google VSAQ

Minimize third-party and internal risks

- Use automation for vendor management
- Reduce the amount of work. Look for control that meets the purpose, they meet controls and documentation level that you expect for your own internal level
- Teeth in the contracts, periodic review
- Breach due to vendor? Data exposed? Show that due diligence was done, appropriate controls where in place and additional security practices where instantiated to protect to the best level of ability and appropriate to the level of sensitivity
- Diversified data stores – pulling data from different IT security applications, everything you said you will do is done, if not, create a gap analysis and remediation plan. Visibility is the key.

Supplier's Management – ISO 27001



Risk Assessment

Screening / Auditing

Selecting clauses in the agreement

Access control

Compliance monitoring

Termination of the agreement

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Cybersecurity and GDPR for M&A

- Why M&A need Cyber Security support?
- What is the impact from the GDPR?
- What value does a security professional bring to the team?

Business Drivers

- Confidentiality
- Speed
- Business as usual
  - Zero Impact
- Informed Business Decision on Risk

M&A Threats

- Special Interest Groups – gain from the Operation
  - Financial Criminals
  - Competitors
  - Acquisition / Merger Company
  - Disgruntled Employees
- General Interest Groups – gain from Impact
  - Script Kiddies / Hackers
  - Hacktivists / Terrorists
  - Spies

This used to be the only threat…

https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html

TECHNOLOGY

The New York Times

Verizon Will Pay $350 Million Less for Yahoo

A Verizon store in Chicago. Verizon will pay $4.48 billion for Yahoo, about $350 million less than it initially offered after security breaches that were disclosed last year.

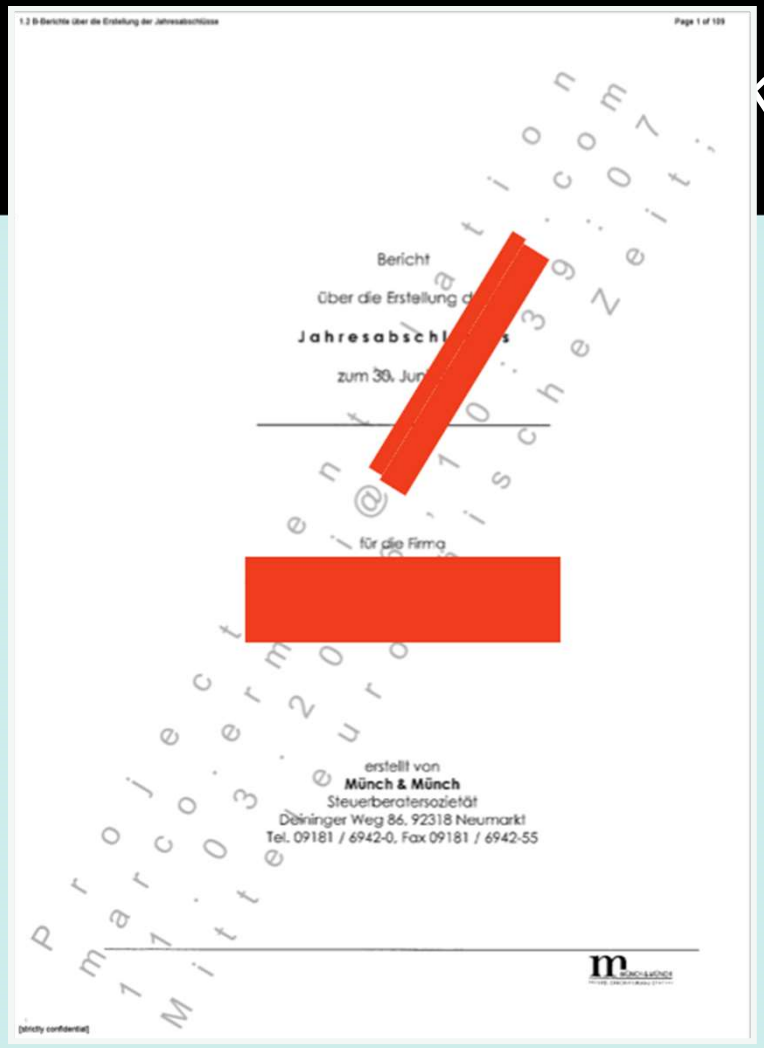
Christopher Dilts/Bloomberg

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Introspection moment

- Publicity, raising profile — your interest gets attacker's interest!
- Impact on:
  - Resources
  - Technologies
  - Infrastructure
- Disgruntled Employees
- Change in threat and risk model
- Absorbing unknown / confusion
- Creating new attack vectors and window of opportunity
- Business drivers force the hand of the Security Manager very quickly
- **Are we all really equipped for change?**

ks for real



1.2 B-Berichte über die Erstellung der Jahresabschlüsse — Page 1 of 109

Bericht

über die Erstellung d

Jahresabschl s

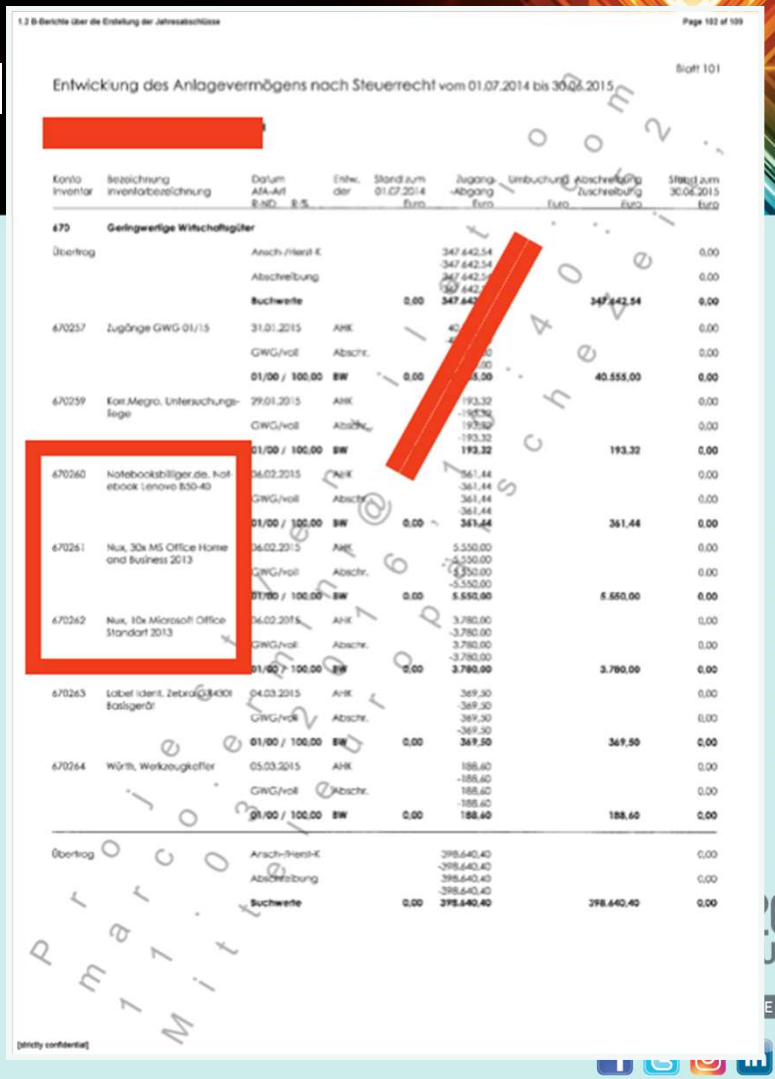
zum 30. Jun

für die Firma

[redacted]

erstellt von
Münch & Münch
Steuerberatersozietät
Deininger Weg 86, 92318 Neumarkt
Tel. 09181 / 6942-0, Fax 09181 / 6942-55

[strictly confidential]



1.2 B-Berichte über die Erstellung der Jahresabschlüsse — Page 102 of 109

Blatt 101

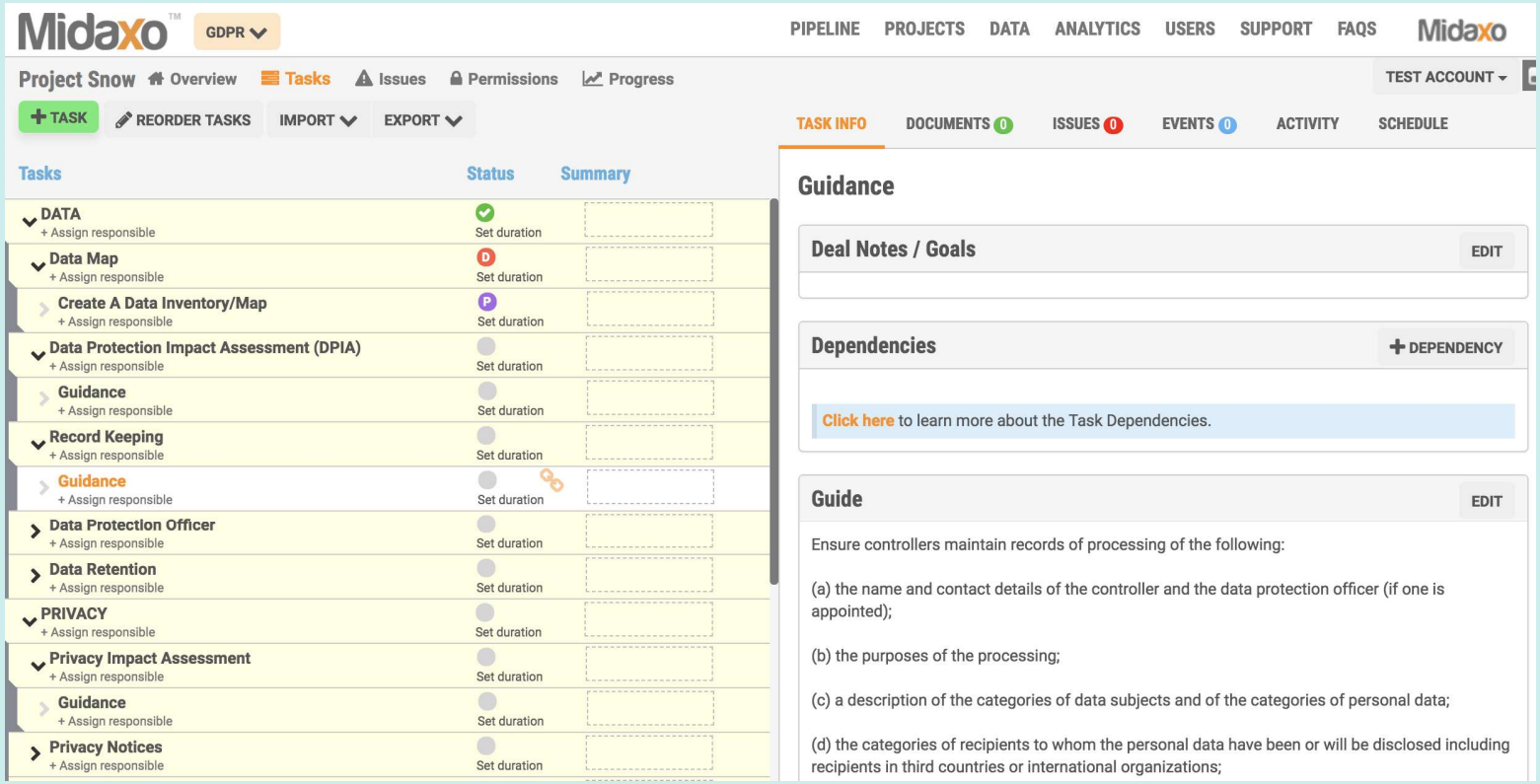
Entwicklung des Anlagevermögens nach Steuerrecht vom 01.07.2014 bis 30.06.2015

[redacted]

Konto Inventar	Bezeichnung Inventarbezeichnung	Datum AfA-Art R-ND R-%	Entw. der	Stand zum 01.07.2014 Euro	Zugang Abgang Euro	Umbuchung Euro	Abschreibung Zuschreibung Euro	Stand zum 30.06.2015 Euro
670	**Geringwertige Wirtschaftsgüter**							
Übertrag		Ansch./Herst.-K.			347.642,54			0,00
		Abschreibung			-347.642,54			0,00
		Buchwerte		**0,00**	**347.642,54**		**347.642,54**	**0,00**
670257	Zugänge GWG 01/15	31.01.2015	AHK		40			0,00
		GWG/voll	Abschr.		-40			0,00
		01/00 / 100,00	**BW**	**0,00**	**40,00**		**40,00**	**0,00**
670259	Kart.Megro, Untersuchungs-liege	29.01.2015	AHK		193,32			0,00
		GWG/voll	Abschr.		-193,32			0,00
		01/00 / 100,00	**BW**		**193,32**		**193,32**	**0,00**
670260	Notebookbilliger.de, Hot eBook Lenovo B50-80	06.02.2015	AHK		361,44			0,00
		GWG/voll	Abschr.		-361,44			0,00
		01/00 / 100,00	**BW**	**0,00**	**361,44**		**361,44**	**0,00**
670261	Nux, 30x MS Office Home and Business 2013	06.02.2015	AHK		5.550,00			0,00
		GWG/voll	Abschr.		-5.550,00			0,00
		01/00 / 100,00	**BW**	**0,00**	**5.550,00**		**5.550,00**	**0,00**
670262	Nux, 10x Microsoft Office Standart 2013	06.02.2015	AHK		3.780,00			0,00
		GWG/voll	Abschr.		-3.780,00			0,00
		01/00 / 100,00	**BW**	**0,00**	**3.780,00**		**3.780,00**	**0,00**
670263	Label Ident, Zebra GK420t Basisgerät	04.03.2015	AHK		369,50			0,00
		GWG/voll	Abschr.		-369,50			0,00
		01/00 / 100,00	**BW**	**0,00**	**369,50**		**369,50**	**0,00**
670264	Würth, Werkzeugkoffer	05.03.2015	AHK		188,60			0,00
		GWG/voll	Abschr.		-188,60			0,00
		01/00 / 100,00	**BW**	**0,00**	**188,60**		**188,60**	**0,00**
Übertrag		Ansch./Herst.-K.			398.640,40			0,00
		Abschreibung			-398.640,40			0,00
		Buchwerte		**0,00**	**398.640,40**		**398.640,40**	**0,00**

[strictly confidential]

Virtual Data Rooms



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

GDPR driving changes in M&A

- Significant behavioural change in acquirers
- Embed GDPR considerations in technology due diligence
- Failing to do this brings significant transaction risks
- Gap Analysis for GDPR readiness
- Key areas: **due diligence** and **post-merger** integration

Due diligence – technical goals

- Actual liabilities in terms of compliance
- How divergent a target is from the buyer's internal processes and standards
  - potential impact on the post-merger roadmap
- Latent security issues in the product/service
  - reputational, operational, financial or legal impact
- Identify risks in:
  - Compliance
  - Market
  - Technical assets including intellectual property
  - Operations
  - Integration

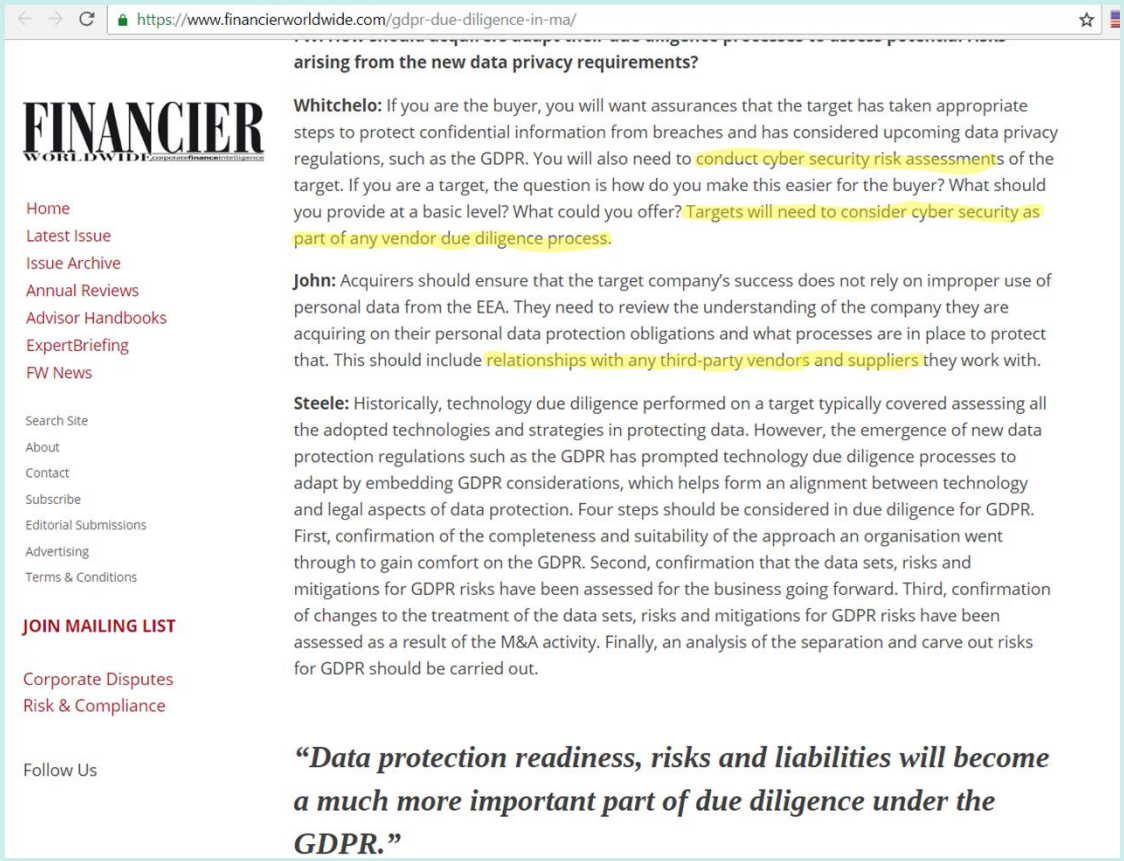
Due diligence risk assessment

- “Privacy risk”
- Much more comprehensive
- How target collects, stores, uses and transfers personal data
- Historical data breaches
- Include data processing in NDAs
- QUIZ time!

Buyer
Target

Data Controller
Data Processor

M&A experts on GDPR and Cybersecurity



https://www.financierworldwide.com/gdpr-due-diligence-in-ma/

arising from the new data privacy requirements?

FINANCIER WORLDWIDE corporatefinanceintelligence

Home
Latest Issue
Issue Archive
Annual Reviews
Advisor Handbooks
ExpertBriefing
FW News

Search Site
About
Contact
Subscribe
Editorial Submissions
Advertising
Terms & Conditions

JOIN MAILING LIST

Corporate Disputes
Risk & Compliance

Follow Us

Whitchelo: If you are the buyer, you will want assurances that the target has taken appropriate steps to protect confidential information from breaches and has considered upcoming data privacy regulations, such as the GDPR. You will also need to conduct cyber security risk assessments of the target. If you are a target, the question is how do you make this easier for the buyer? What should you provide at a basic level? What could you offer? Targets will need to consider cyber security as part of any vendor due diligence process.

John: Acquirers should ensure that the target company's success does not rely on improper use of personal data from the EEA. They need to review the understanding of the company they are acquiring on their personal data protection obligations and what processes are in place to protect that. This should include relationships with any third-party vendors and suppliers they work with.

Steele: Historically, technology due diligence performed on a target typically covered assessing all the adopted technologies and strategies in protecting data. However, the emergence of new data protection regulations such as the GDPR has prompted technology due diligence processes to adapt by embedding GDPR considerations, which helps form an alignment between technology and legal aspects of data protection. Four steps should be considered in due diligence for GDPR. First, confirmation of the completeness and suitability of the approach an organisation went through to gain comfort on the GDPR. Second, confirmation that the data sets, risks and mitigations for GDPR risks have been assessed for the business going forward. Third, confirmation of changes to the treatment of the data sets, risks and mitigations for GDPR risks have been assessed as a result of the M&A activity. Finally, an analysis of the separation and carve out risks for GDPR should be carried out.

"Data protection readiness, risks and liabilities will become a much more important part of due diligence under the GDPR."

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Engage cybersecurity risks for GDPR in M&A

- Engage cybersecurity experts

- New questions
  - How is cyber-diligence conducted?
  - Specialist service providers?
  - What do we need to be aware of?
  - Has the business enough technical knowledge?

Four Steps for Due Diligence

- Completeness and suitability of the approach of target
- Data sets, risks and mitigations for GDPR risks have been assessed
- Changes to the treatment of the data sets, risks and mitigations for GDPR risks have been assessed as a result of the M&A activity
- Analysis of the separation and carve out risks for GDPR

Post-Merger activities – Basics

- Capture
- Connect
- Combine
- Consolidate

Post-Merger activities – GDPR specifics

- Address consent from existing Data Subjects
- Security Transformation Program
- Manage risk in the short/medium term while satisfying compliance
- Ensure detect and respond strategy for cyber security incidents
- Technical Security consulting in cyber security

The Role of the Cybersecurity Expert

- Protecting the effort itself
  - Confidentiality of the total effort
  - Confidentiality of the team's work
- Evaluating the security condition of the target company
  - Impact on the deal's value – GDPR into play
  - Asking the right questions
- Providing subject matter expertise
  - Identify Security Requirements for the New Company
  - Controlling Rumors
  - Managing Global/International Aspects
  - "Team Consultant"
  - Low Hanging Fruits

The Cybersecurity Expert in action

- Preliminary background investigations
  - Collection of Open-Source information
- Due diligence
  - More in-depth look
  - Estimation of Costs of Cyber Security – GDPR impact!
- Operations security – post-merger into focus
  - Protect operational activities
  - Develop and implement protective measures
  - Appropriate for each phase of the acquisition

Combining the two companies

- Resources, staffing, processes, and systems
- Business processes
- IT tools
- ***Active Directory merging strategy is key!***
- The Target company has comparable / same security
- Exceptions are documented and signed off by leadership
- Agreed-upon designs
- Operations turned to standard support
- Weekly or recurring meetings

IT/Cybersecurity Post-Mergers Objectives

Target Characteristics	Security Guidelines	SLAs
SMALL ➢ Small employee base (< 200 employees) ➢ Low complexity ➢ Private ownership ➢ Little to no geographical diversity ➢ No separate legal entities ➢ No/limited need to keep the same facilities ➢ No/limited to keep the existing technologies ➢ Purchased for limited product portfolio, technology, talent, or local presence	➢ Baseline security controls Target is fully absorbed into IT infrastructure ➢ All IT labor is absorbed into IT global business units	➢ Security controls established or confirmed in less than 100 days
MEDIUM ➢ Similar to previous kind, but Target has certain identifiable complexities that require specific sensitivity during integration ➢ Fewer than 500 employees ➢ Needs to be stand-alone for a certain period of time ➢ During stand-alone time, Target maintains defined non-compliances ➢ Supports its own IT infrastructure during the stand-alone phase	➢ Integration of Target may be full, hybrid, or standalone ➢ All IT labor is absorbed into IT global business units	➢ Operation integration of some IT infrastructure may take +180 days ➢ Processes may take 3 to 9 months
LARGE ➢ More than 500 employees ➢ Relatively large operations ➢ Significant multinational presence and subsidiaries ➢ Target contains certain identifiable complexities that require specific sensitivity during integration	➢ Integration of Target may be full, hybrid, or standalone ➢ IT labor can stay funded by Target company	➢ Operation integration of some IT infrastructure may take +180 days ➢ Customized integration plan ➢ IT Support is shared ➢ Processes take more than 12 months

Merging Policies

- Safeguards against disgruntled employees
- New employee contracts
  - Are existing Policies still relevant?
  - Are we “dumbing down” their security?
- Existing employee contracts
  - Do they protect you?
  - Do they meet new relationship?
- Identify key policies — yours vs theirs
  - Work with Legal Departments

Conclusions

- Lack of privacy documentation can lower target's value
- Privacy by design and by default can have business fall behind
- "Personal information is the new gold"
- Strategy for cost-effective data protection =
  - Competitive advantage
  - Boost in value
  - Considered more secure trustworthy by customers
  - Emphasize valuation
- Rewards in greater utilization of personal data
- **Potential reward: increase M&A deal value significantly**

GDPR has no specific guidance on Cloud

- Using Cloud Services invokes a shared responsibility model
- GDPR creates issues for organizations that process personal data in the Public Clouds
  - rights of data subjects
  - data residency
  - cross-border transfers
- The level of support from cloud providers may not be known
- Recommendations:
  - gap analysis
  - identify the organizational and technical actions required
  - ask all public cloud service providers to provide required certification or proof of adherence to a code of conduct

Helpful Cloud tools

- A Data Controller is responsible for the conduct of any of its Data Processors – even if they are Cloud Providers
- Noncompliance with regard to GDPR on the vendor side reflects on the compliance of the end-user organization
- Moving to the cloud may add to the security aspects of the processing activity, but could also lead to residency concerns
- CASB service may be helpful
- Data protection in hybrid or on-premises operations is increased by adoption of DCAP products
- Privacy compliance is demonstrated by mapping, dashboarding and logical control application

Cloud IaaS and GDPR

- IaaS cannot make a company GDPR-compliant, but can help
- On their own, Clouds' behaviour and tools will be insufficient
  - Google and Microsoft have specific awareness of user-generated personal data
  - AWS currently offers this in a limited way with Amazon Macie
- Recommendations
  - Perform a DPIA when selecting a Cloud Provider
  - Perform a DPIA for each business process using a Cloud Provider
  - Use Cloud-provided tools when the risk assessment identifies that they can adequately address that part of the GDPR problem

Implementing a GDPR program

Can I insure against GDPR violations?

What cannot be insured

- Generally, any fine
  - especially if connected to deliberate recklessness or connected to a criminal offence
- Customer's churn
- An insurer may not be liable for payment of indemnity in certain circumstances

What can be insured

- Costs of investigating an incident
- Defence costs
- Claims by third parties (customers and suppliers) for consequences of a breach
- Costs of mitigating a breach – including public relations (e.g. notification) expenses

In certain countries, GDPR fines *may* be insurable

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

GDPR Regulatory Heat Map

Not insurable

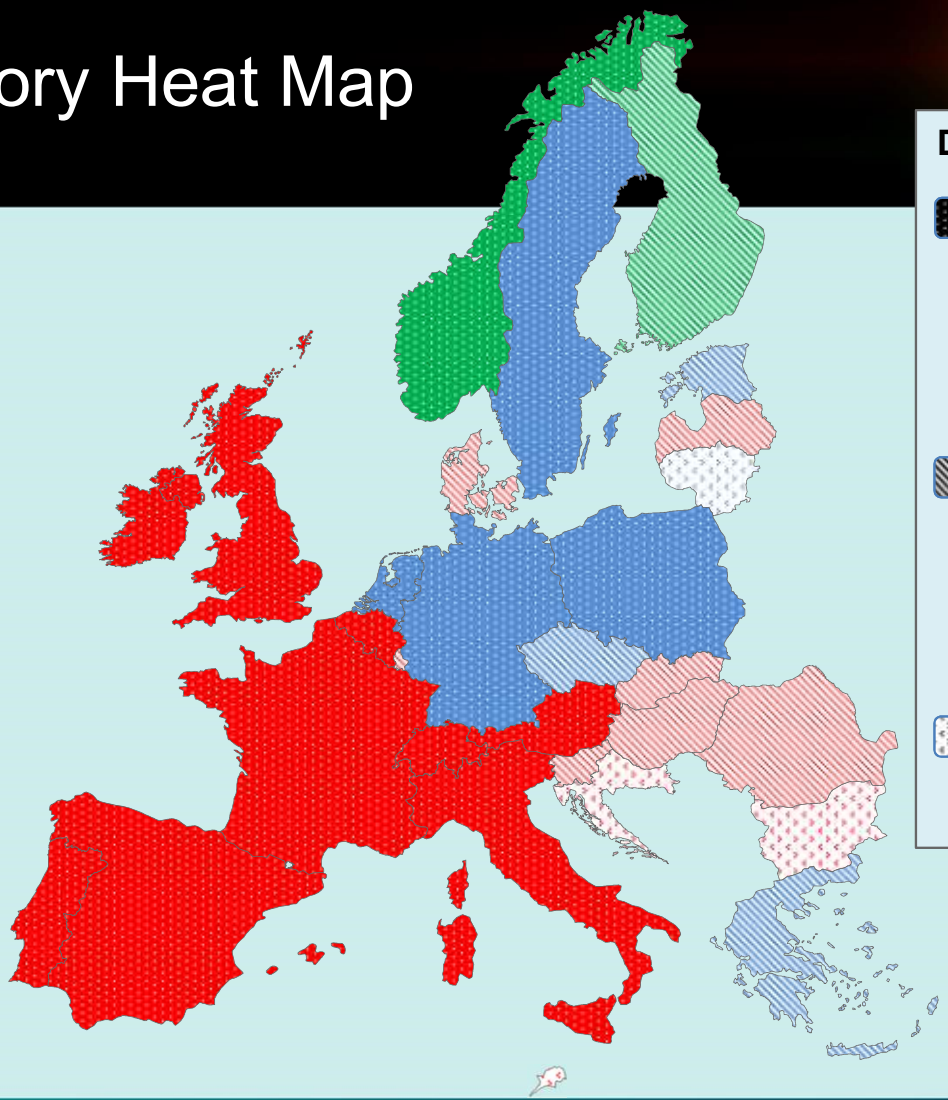
Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, France, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Portugal, Romania, Slovakia, Spain, Switzerland, United Kingdom

Unclear

Estonia, Germany, Greece, Netherland, Poland, Lithuania, Sweden

Insurable

Finland, Norway



Data Regulatory Environment

High
Austria, Belgium, France, Germany, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland

Fairly High
Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Latvia, Luxembourg, Romania, Slovakia, Slovenia

Moderate
Bulgaria, Croatia, Lithuania, Malta

Source: DLA Piper (update 2018)

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Three dimensions of continuous improvement

Security Processes

Risk Management
Information Lifecycle
Privacy by Design
Privacy by Default
Data Discovery & Classification
Asset Management
Physical Security
Change Management
Incident Response
Breach Notification
Compliance Programs
Vulnerability Management
Third-party Management
Documentation Management

Technical Measures

Access Control
Data Deletion
Encryption
Pseudonymisation (Data Masking)
Monitoring
Secure Configuration
DR/BCM
Application Security
Data Leakage Prevention
Content Filtering

Organizational Measures

Employment Procedures
Confidentiality Agreements
Security & Privacy Awareness
Acceptable Use Policy
Access Controls

Selected Controls Supporting GDPR Activities

Consent Management

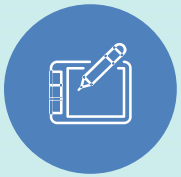
Art. 7

Data Portability

Art. 20

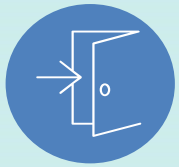
Record of Processing Activities (ROPAs)

Art. 30



Data Privacy Impact Assessment (DPIA)

Art. 35



Right to Access

Art. 15

Protection by Design and Default

Art. 25

Continuous Compliance

Art. 32

International Data Transfer

Art. 44-46

Ability to Erase Personal Data

Art. 17

Pseudonymisation (Data Masking)

Art. 6
R. 26, 28

Breach Notification

Art. 33, 34

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Encryption and Pseudonymisation

- Encrypted data usually leads to pseudonymisation
  - Re-identification and decryption after a data breach are still a risk
- Anonymise means delete or change identification marks so that re-identification is impossible
- Pseudonymisation means prevent identification of the individual by unauthorized parties or render such identification difficult
- Pseudonymisation can include data masking, redaction, tokenization and/or encryption
- Ways to enhance security, but do not necessarily create data that is out of scope for the GDPR
- Data breaches on encrypted personal data should be still reported to regulatory authority

Data Masking

- Two main reasons to use data masking

1. personal identifiable data can only be used for designated purposes

2. masking reduces risk/impact from a data breach

Tokenisation vs Encryption

Tokenisation	Encryption
Output is format and length preserving	Output is generally not format length preserving, except for FPE/OPE
May or may not use encryption as mapping function (can use hashing as mapping table)	Encryption does not have any use for tokenisation
Output may or may not be reversible	Given the key, output is always reversible
PCI DSS, GDPR	GDPR, HIPAA
Main use case: reduce PCI scope	Main use case: confidentiality of data at rest

Consent Management Tools

- Standards are lacking
- Building trust-based relationships between consumers and brands that put consumers in control of their personal data.
- Key to avoid the high costs of noncompliance
- It will likely be absorbed into consolidated marketing suites
  - Document precise user experience (UX) requirements
  - Develop a granular consent matrix
  - Provide a customer consent dashboard
  - Determine if a packaged consent management solution is justified
  - Implement formal review and approval for consent flow designs
  - Prototype with designers and customer experience experts
  - Designs soliciting consent where its value is clear to users

Identity and Access Management

- Heart of data compliance strategy
- Central SSO management is critical for Cloud control
  - “GDPR policy”
  - Multi-factor authentication
  - Restrict contractors/externals
  - Geographical policies
- Can be paired with a CASB product

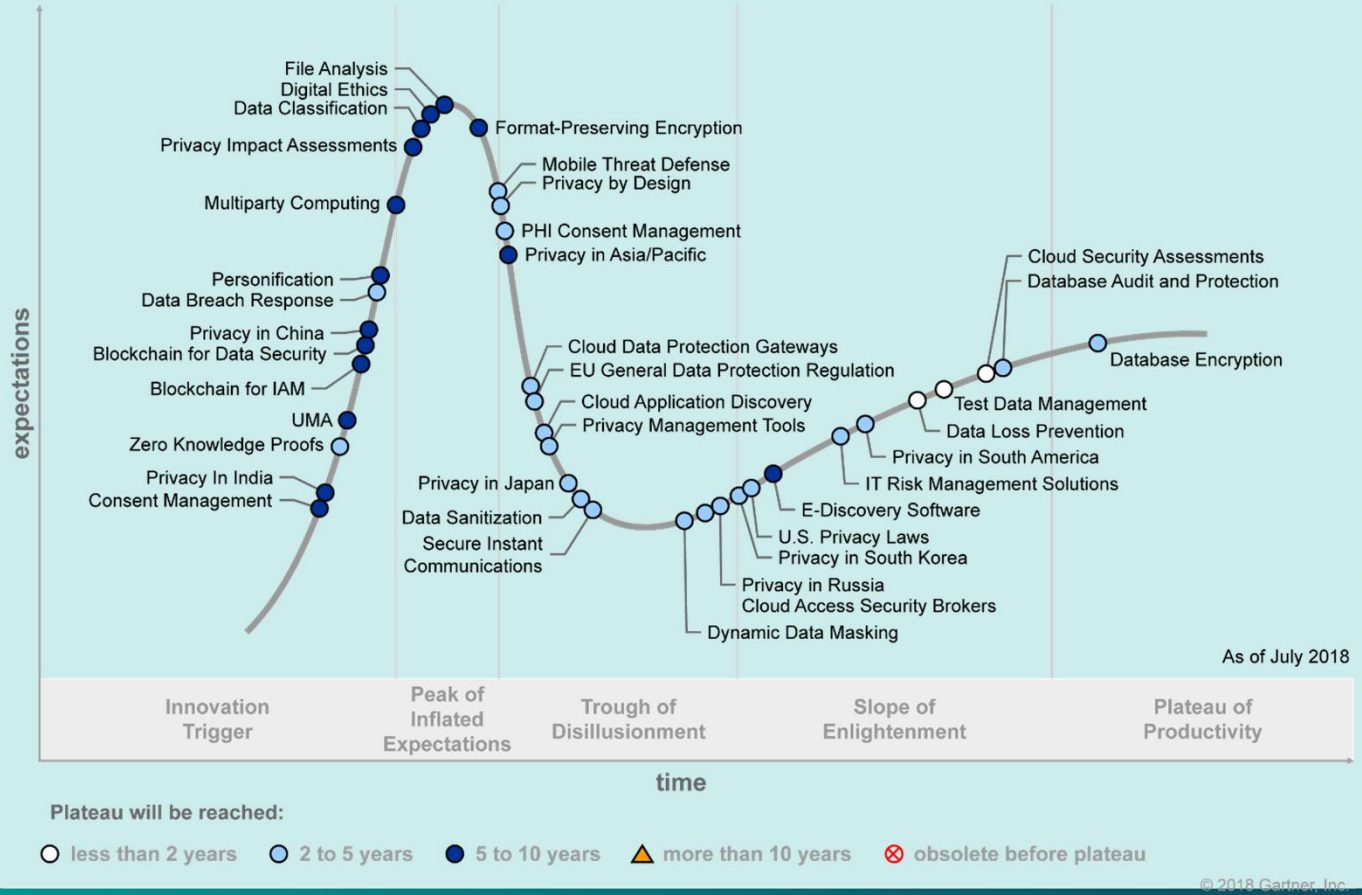
Zero Knowledge Proofs

- "Privacy-preserving messaging protocols that enable entities to prove that information available to both of them is correct, without the requirement to transmit or share the underlying information"
- Characteristics
  - A) Completeness – encoding as a polynomial problem
    - The prover wants to convince the verifier that this equality holds
  - B) Succinctness by random sampling
    - Reduces both the proof size and the verification time tremendously
  - C) Homomorphic encoding / encryption
    - Allows proving E(func(s)) without knowing s
  - D) Zero Knowledge
    - The prover obfuscates in a way that the verifier can still check their correct structure without knowing the actual encoded value

Zero Knowledge Proofs – user advice

- Gain a deeper understanding of the nature of these controls
- Be realistic with the current immaturity of ZKP solutions
- Evaluate how such controls may impact transaction authentication and ultimately consumers
- Assess the impact on the broader information management strategy
- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers

“Hype-Cycle” of GDPR



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Privacy Officers

- Preparatory plan
- Build relationships
  - Identify stakeholders
  - Campaign internally
  - Increase organizational understanding
  - Map out a plan for the future
- Establish the Privacy Program
  - Maintain privacy documentation for business units and users
  - Establish a companywide mandatory reporting mechanism
  - Review existing personal-data-processing operations
  - Prioritize actions
- Keep reputation for integrity, inside and outside the company

Incident Management

Recent Incidents

TC

Startups
Apps
Gadgets
Events
Videos

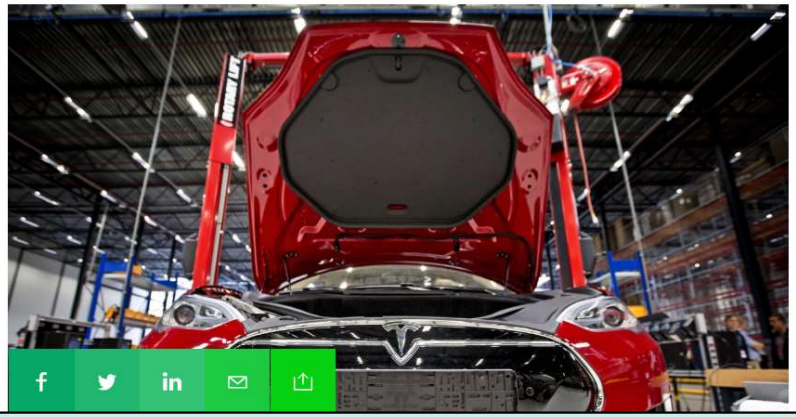
Crunchbase
More

Search

Disrupt SF 2018
Gaming
Apple
Transportation

Data breach exposes trade secrets of carmakers GM, Ford, Tesla, Toyota

Kirsten Korosec @kirstenkorosec / Jul 21, 2018 Comment

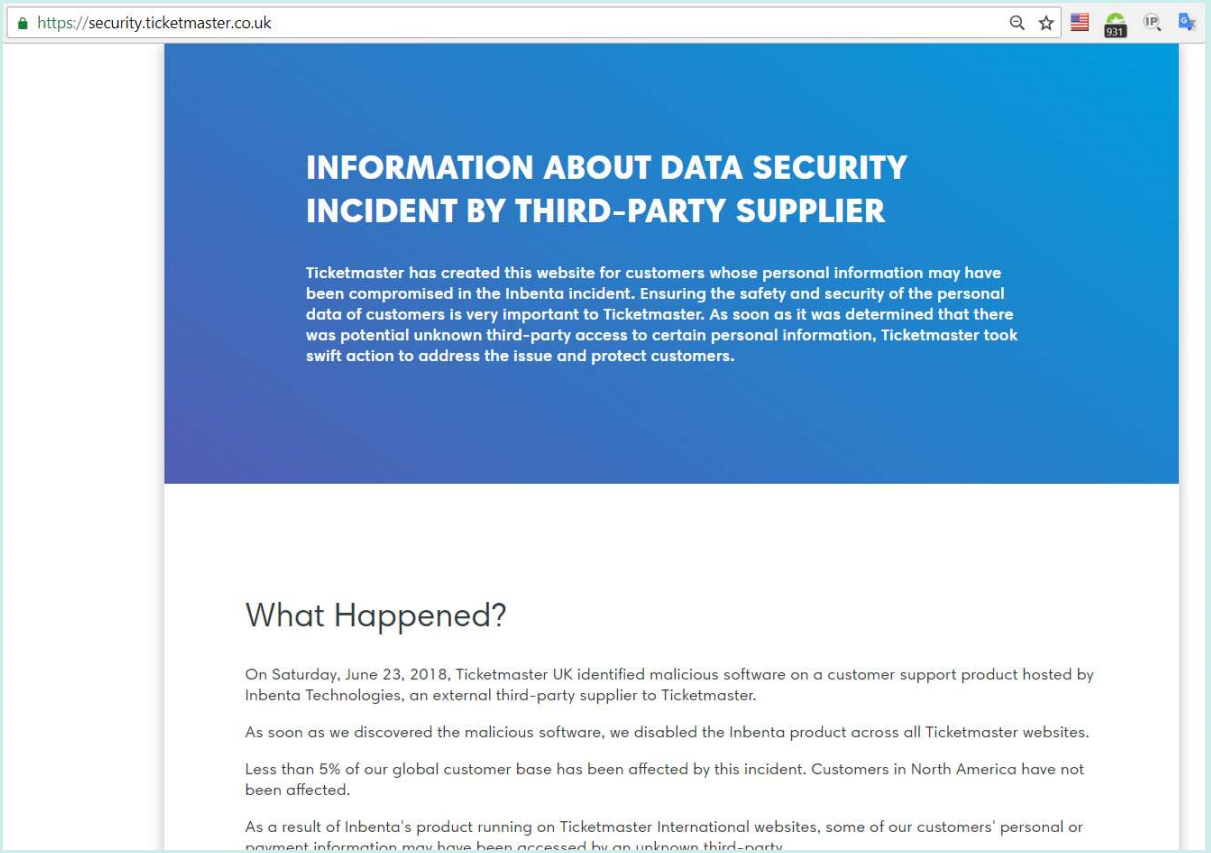


The New York Times

'Big Red Flag': Automakers' Trade Secrets Exposed in Data Leak

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Recent Incidents



Reporting to the CFO and Potential Investors

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Key Findings from breached companies

- Shares hit low point approximately 14 market days after breach
  - share prices -2.89% on average, underperform NASDAQ by 4.6%
- After about a month, share prices rebound and catch up to NASDAQ performance
- After first month, companies performed better than prior breach
  - six months before breach, average share price +3.64%, but is +7.02% after breach
  - underperformed the NASDAQ by 1.53% before breach, outperform it by 0.09% afterward
- Finance and payment companies have largest drop in share price performance, Healthcare companies are the least affected
- Highly sensitive information see larger drops in share price

Dealing with a Breach

- Plan for a security incident.
- Determine and document your response priorities and escalation paths.
- Brainstorm with members of the organization to think through various scenarios.
- Draft messaging and corporate communications based on the scenarios.
- Know which vendors are material to your operations.
- Make sure that those involved in the response know what their roles will be and what authority they hold. Document it.
- Exercise the plan at least twice per year — preferably quarterly. The more realism you inject into the exercise, the more likely it will execute smoothly in real life.

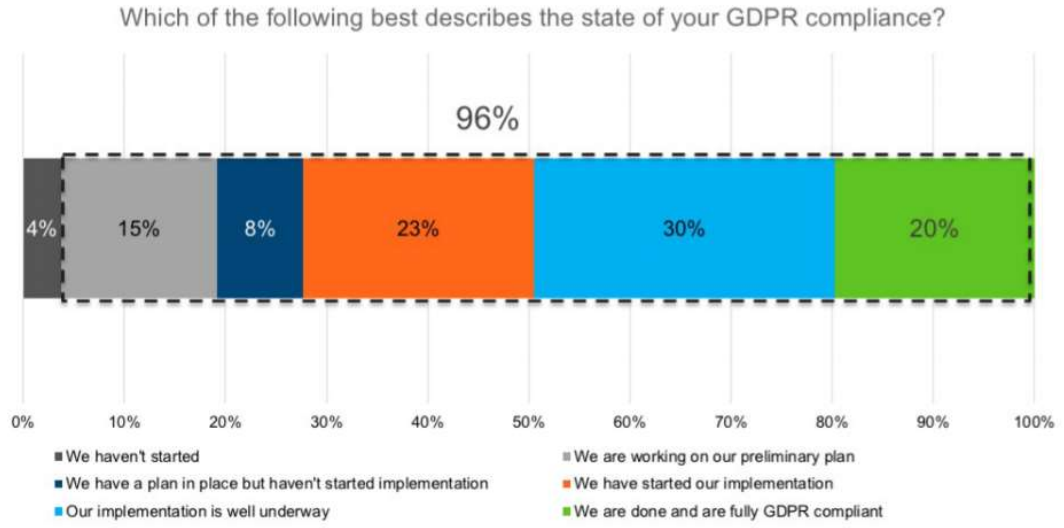
Backup Slides

Backup Slides

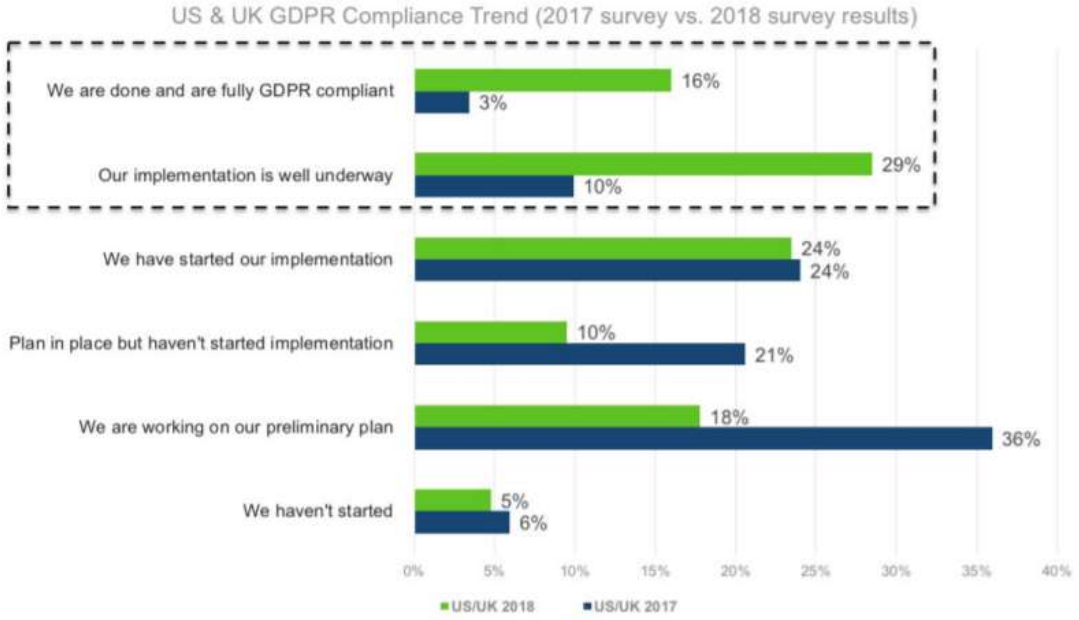
GDPR Implementation Landscape

GDPR compliance is still a work in process

96% have started, but only 20% are fully compliant



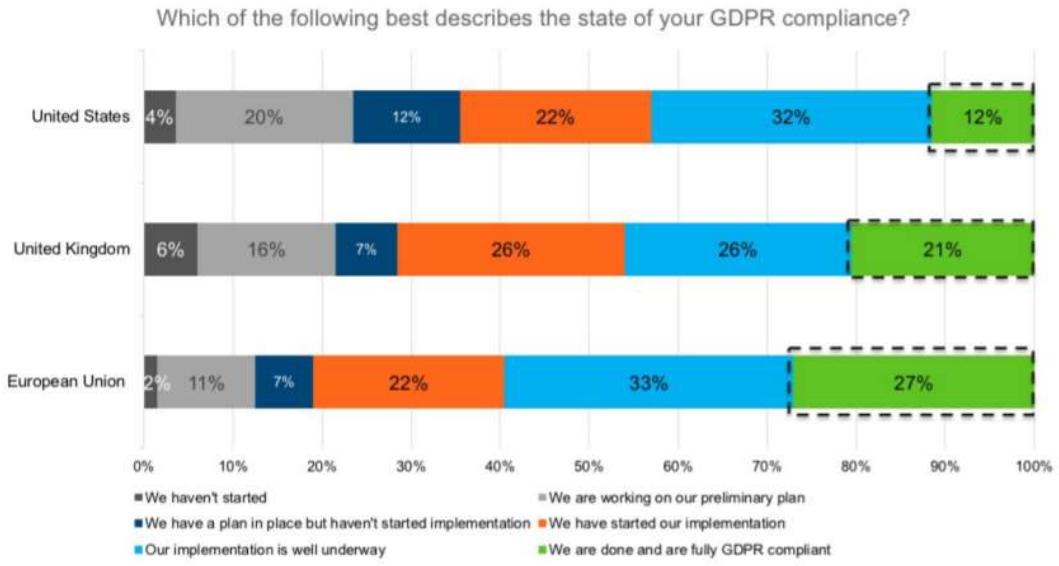
US and UK companies have made good compliance progress in the past year



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

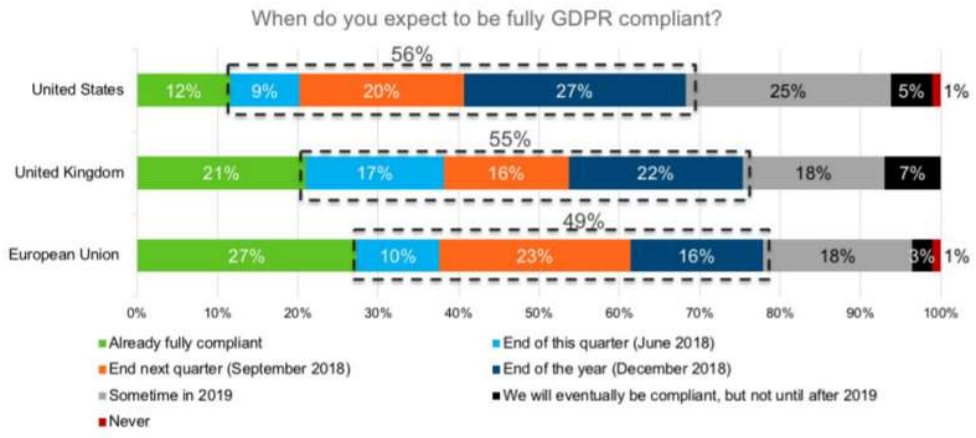
EU slightly ahead of UK and 2X ahead of US

27% in the EU are fully compliant versus only 12% in the US



Many companies expect to become GDPR compliant later this year

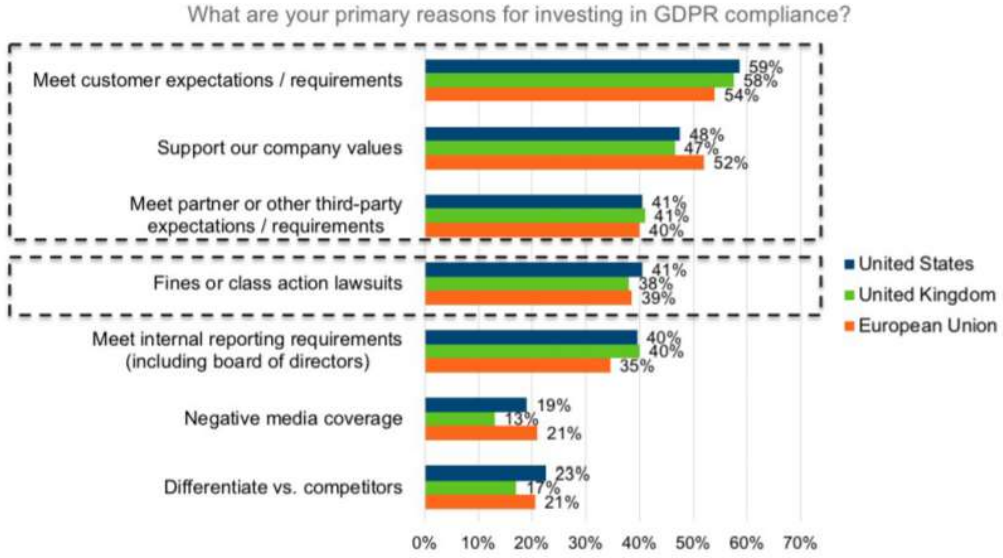
Compliance plans for companies non-compliant as of June 2018:
56% of US companies, 55% of UK companies, and 49% of EU companies expect to become GDPR compliant by the end of 2018



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

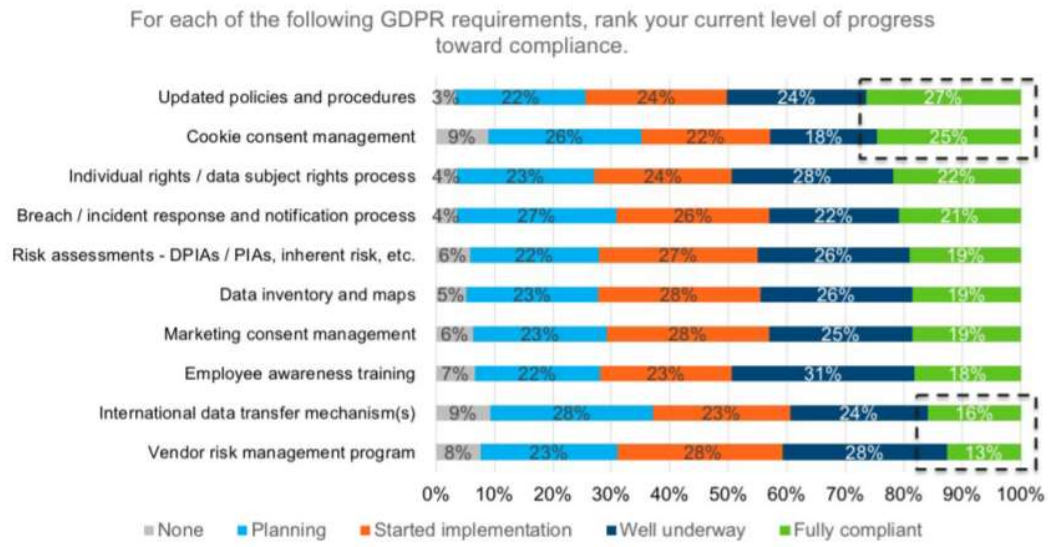
Reasons for investing in GDPR compliance consistent across regions

Motivated more by values, customer and partner expectations than fear of fines



Key GDPR requirements have varying levels of progress

Policy updates, cookie consent most advanced (27% / 25% fully compliant)
Vendor risk, data transfer least advanced (13% / 16% fully compliant)

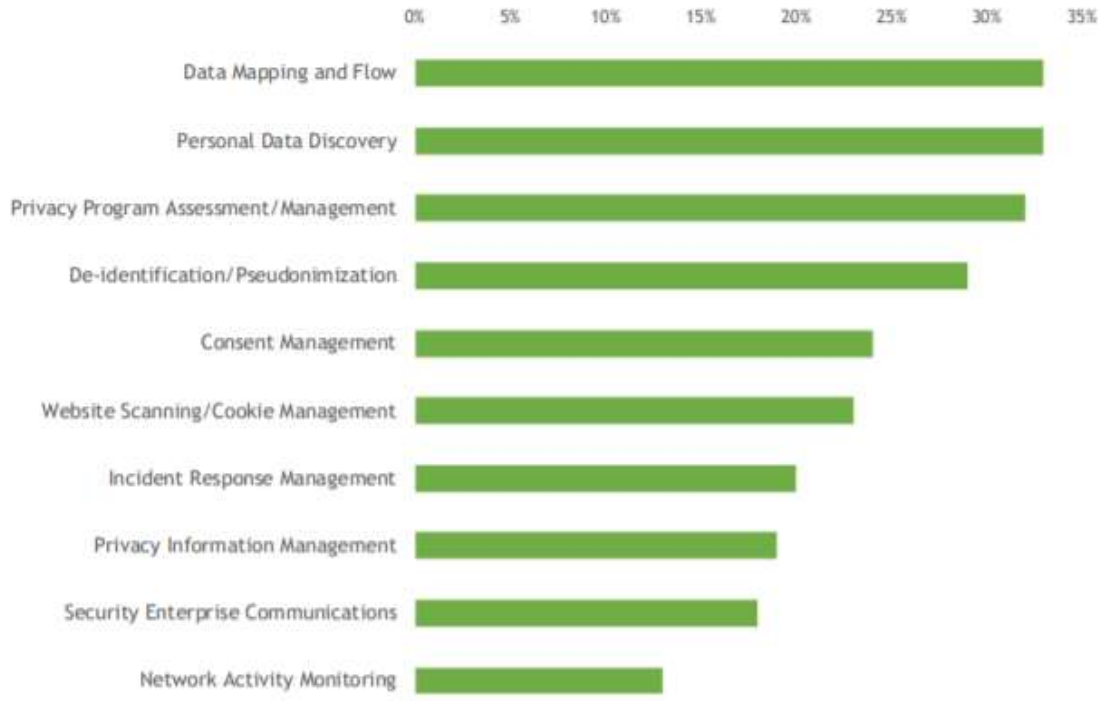


CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

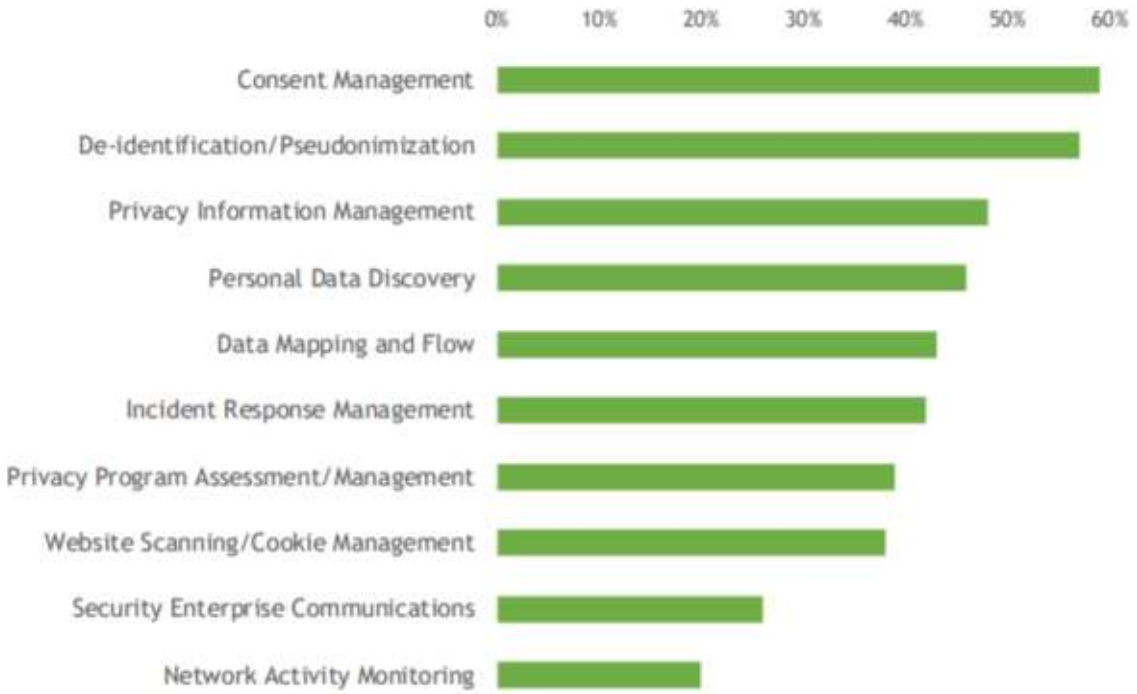
ORGANIZATIONS THAT HAVE PURCHASED AND IMPLEMENTED:

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

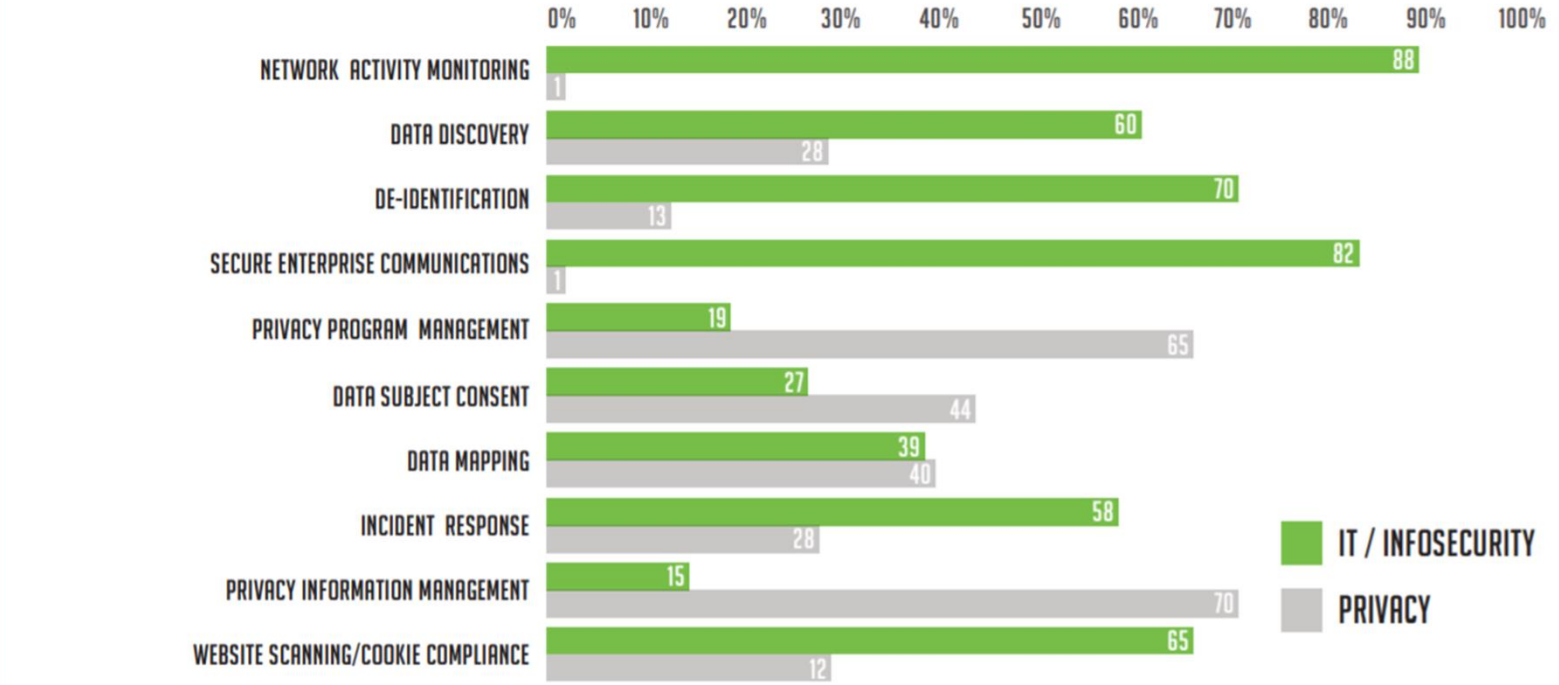
WHAT'S NEXT? ORGANIZATIONS THAT ARE PLANNING TO PURCHASE, OR HAVE PURCHASED BUT NOT IMPLEMENTED:



NICHE MARKETS? ORGANIZATIONS THAT HAVE NOT PURCHASED AND HAVE NO PLANS TO BUY:



WHERE BUDGET FOR PURCHASE RESIDES:

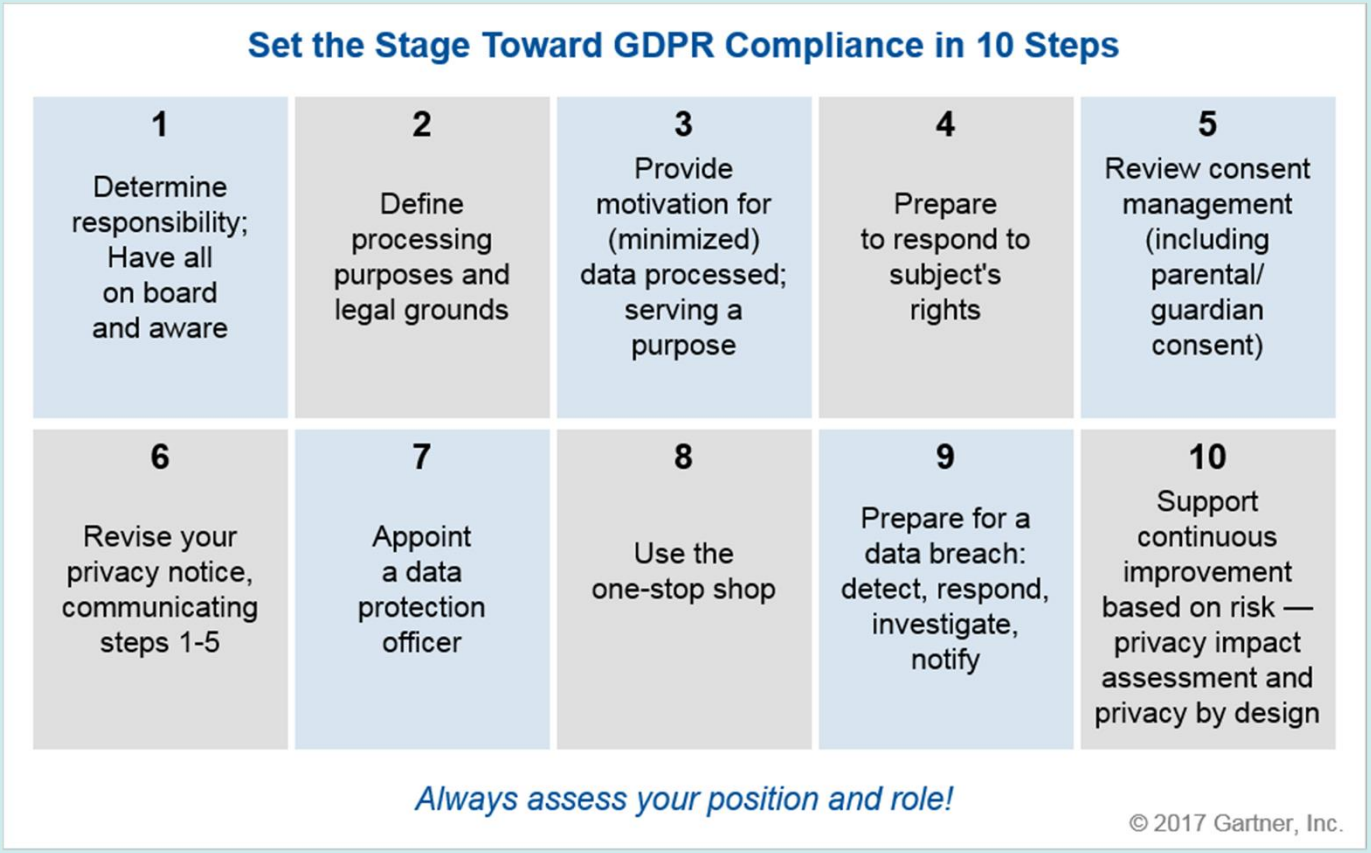


CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Practice Validation Requirements

Data Necessity	Use, Retention, & Disposal	Onward Transfer & Third Parties	Choice & Consent	Access & Individual Rights	Data Quality, Integrity & Security	Transparency	Monitoring & Assurance
1. Data minimization 2. Data protection by design 3. Data protection by default	4. Purpose limitation 5. Data retention 6. Lawfulness of processing 7. Processing of sensitive PI 8. Define and communicate retention periods	9. Evaluate processors 10. Contracts with processors 11. Conduct due diligence of third party controllers 12. Contracts with controllers 13. International data transfer	14. Consent to processing of PI 15. Consent to processing of sensitive PI 16. Consent to international data transfer 17. Provide mechanism to obtain consent 18. Mechanism to withdraw consent 19. Record evidence of consent 20. Obtain parental consent to process children's PI	21. Right of access 22. Right to rectification 23. Right to erasure 24. Right to restrict processing 25.Right to object 26. Rights around use of PI for automated decisioning 27. Rights around using sensitive PI for automated decision-making 28. Right to data portability	29. Complete and accurate data relevant to the processing purpose 30. Security of processing 31. Proportional safeguards 32. Employee awareness 33. Detection of breach incidents 34. Security risk assessments	35. Privacy notice when PI is collected directly from individuals 36. Privacy notice when PI is not collected directly from individuals 37. Notification of changes 38. Breach incident notification 39. Notification of alternative dispute resolution 40. Provision of privacy notice 41. Timing of privacy notice	42. Review of business process activity risk and controls by DPO or privacy office 43. Process to obtain feedback from Individuals whose data is processed by the business activity and other experts 44. Process to integrate individual and expert feedback into technology and business activity design

Gartner's Recipe for GDPR Compliance



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Gartner's Priority Matrix for GDPR

Priority Matrix for Privacy, 2018

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational				
high	**Cloud Security Assessments** **Test Data Management**	Cloud Access Security Brokers Cloud Data Protection Gateways Data Breach Response Database Audit and Protection EU General Data Protection Regulation IT Risk Management Solutions Privacy in Russia Privacy in South Korea Privacy Management Tools U.S. Privacy Laws	Blockchain for Data Security Blockchain for IAM Data Classification Digital Ethics E-Discovery Software File Analysis Multiparty Computing Personification Privacy Impact Assessments Privacy in Asia/Pacific Privacy in China	
moderate	Data Loss Prevention	Cloud Application Discovery Data Sanitization Database Encryption Dynamic Data Masking Mobile Threat Defense PHI Consent Management Privacy by Design Privacy in Japan Secure Instant Communications Zero Knowledge Proofs	Consent Management Format-Preserving Encryption Privacy In India UMA	
low		Privacy in South America		

As of July 2018