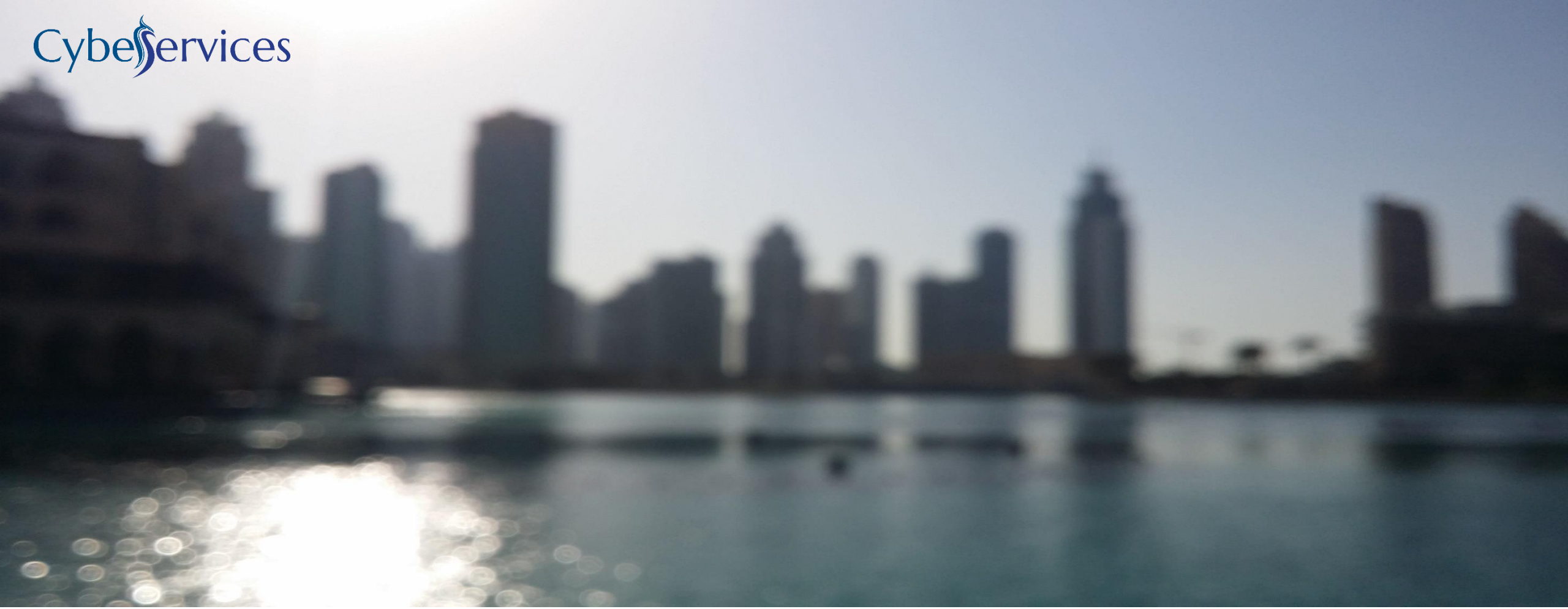


The Talk: Review and Move Forward with GDPR
25 June 2018 (1 month after implementation)

Anett Mádi-Nátor, VP, Cyber Services

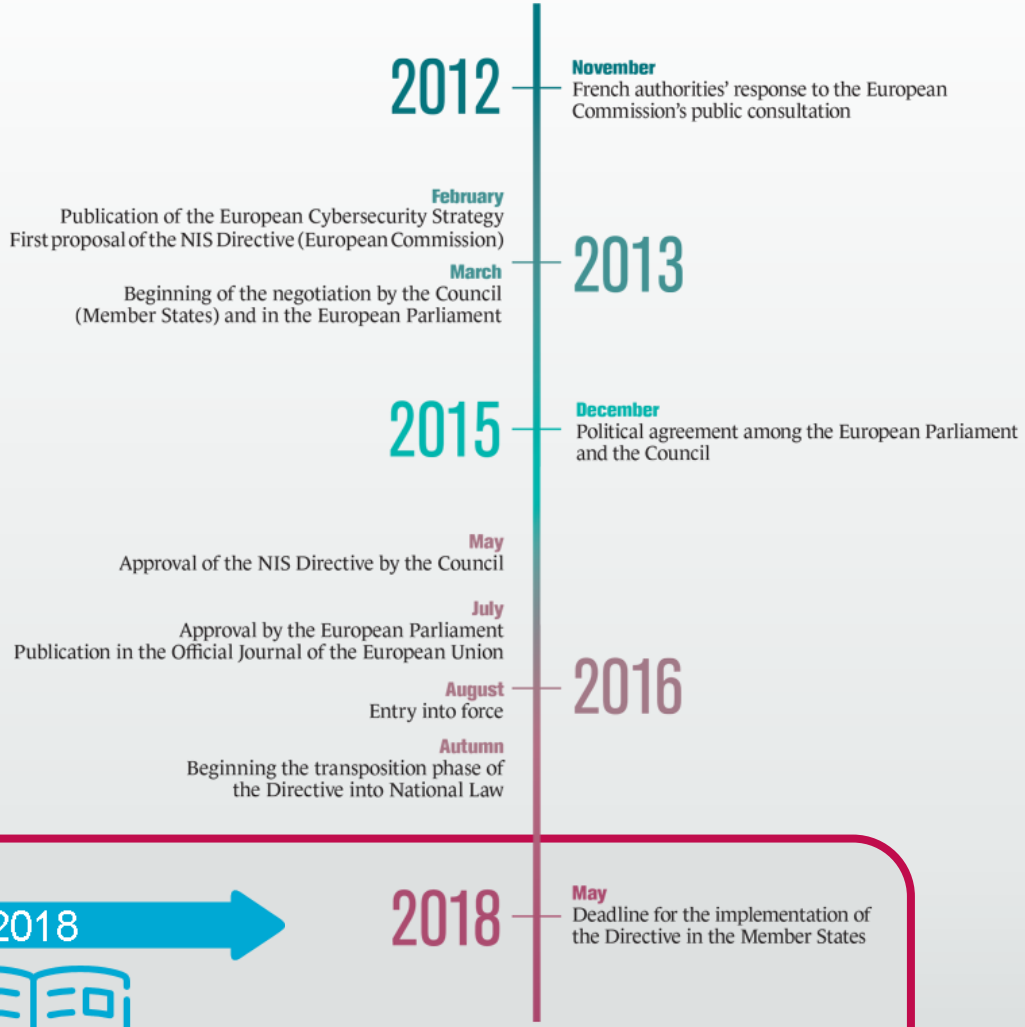
The context - Actual Cyberspace Related Trends in EU

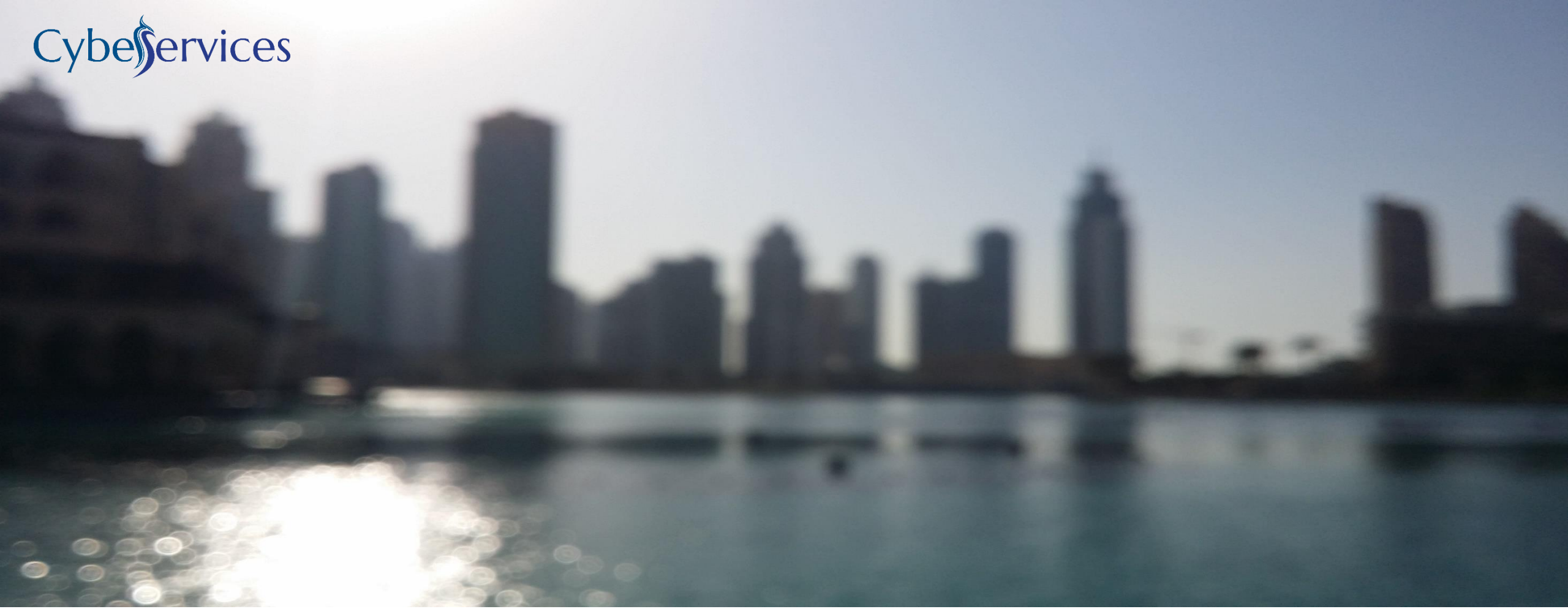
- **Cybersecurity Strategy of the EU**: An Open, Safe and Secure Cyberspace of 7 February 2013;
- Concerning measures for a high common level of security of network and information systems (**NIS**) across the Union of 6 July 2016 (EU 2016/1148);
- The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**GDPR** - EU 2016/679);
- Electronic identification and trust services for electronic transactions in the internal market (**eIDAS** – EU No 910/2014);
- A **Digital Single Market Strategy** for Europe of May 2015;
- **Contractual** Public Private Partnership on Cybersecurity.

Timeline – NIS Directive and GDPR

The **GDPR** must be binding and directly applicable to all Member States.

Definitions of **NIS Directive** will be applied to the member states' national legislations, so it must be applied in the Hungarian legal system too. The complete implementation of the Directive will begin in 2018 May.





The EU General Data Protection Regulation

GDPR – General Data Protection Regulation

12 steps

The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

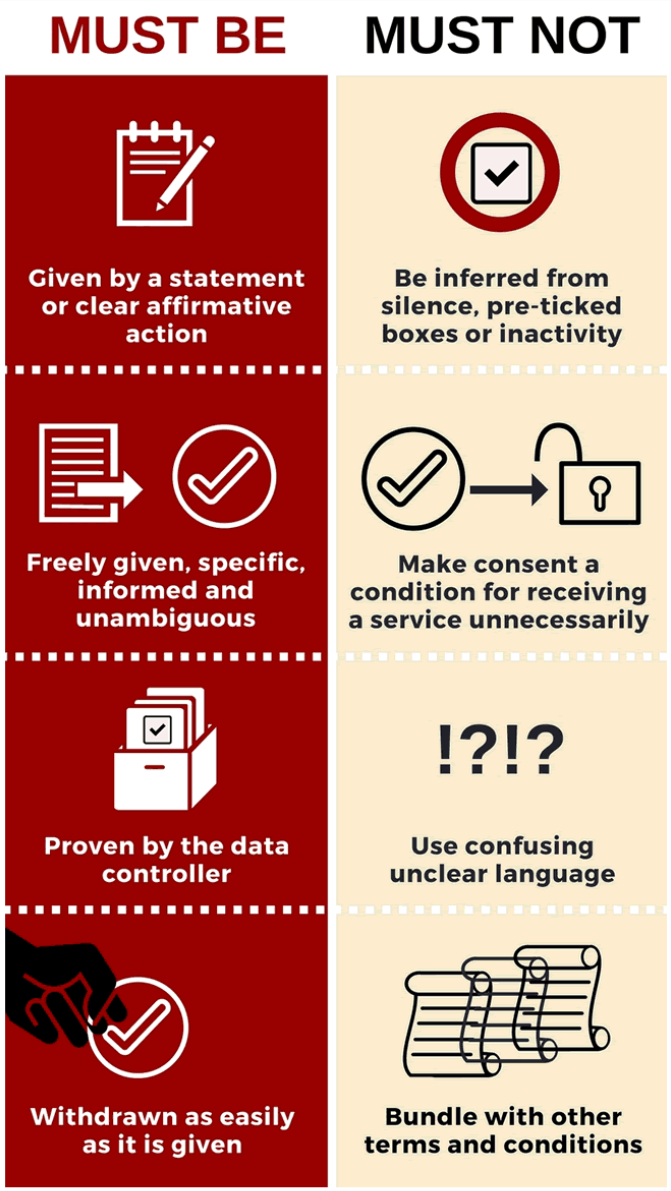
Step 4: Individual Rights

The GDPR provides the following rights for **individuals**:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

This part of the guide explains these rights.

Step 7: Consent



Some GDPR consent elements in a nutshell – source and more info FOIMan

In addition to the existing requirement that consent is freely given, specific and informed, consent must be 'unambiguous' and given 'by a statement or clear affirmative action.'

The GDPR introduces a number of other changes:

Unbundled – consent should be set out separately from the acceptance of other terms and conditions requests.

Active opt-in – organisations must use unticked boxes or similar. Pre-ticked boxes or the requirements to opt out will generally be invalid.

Granular – separate consent should be sought for different types of processing.

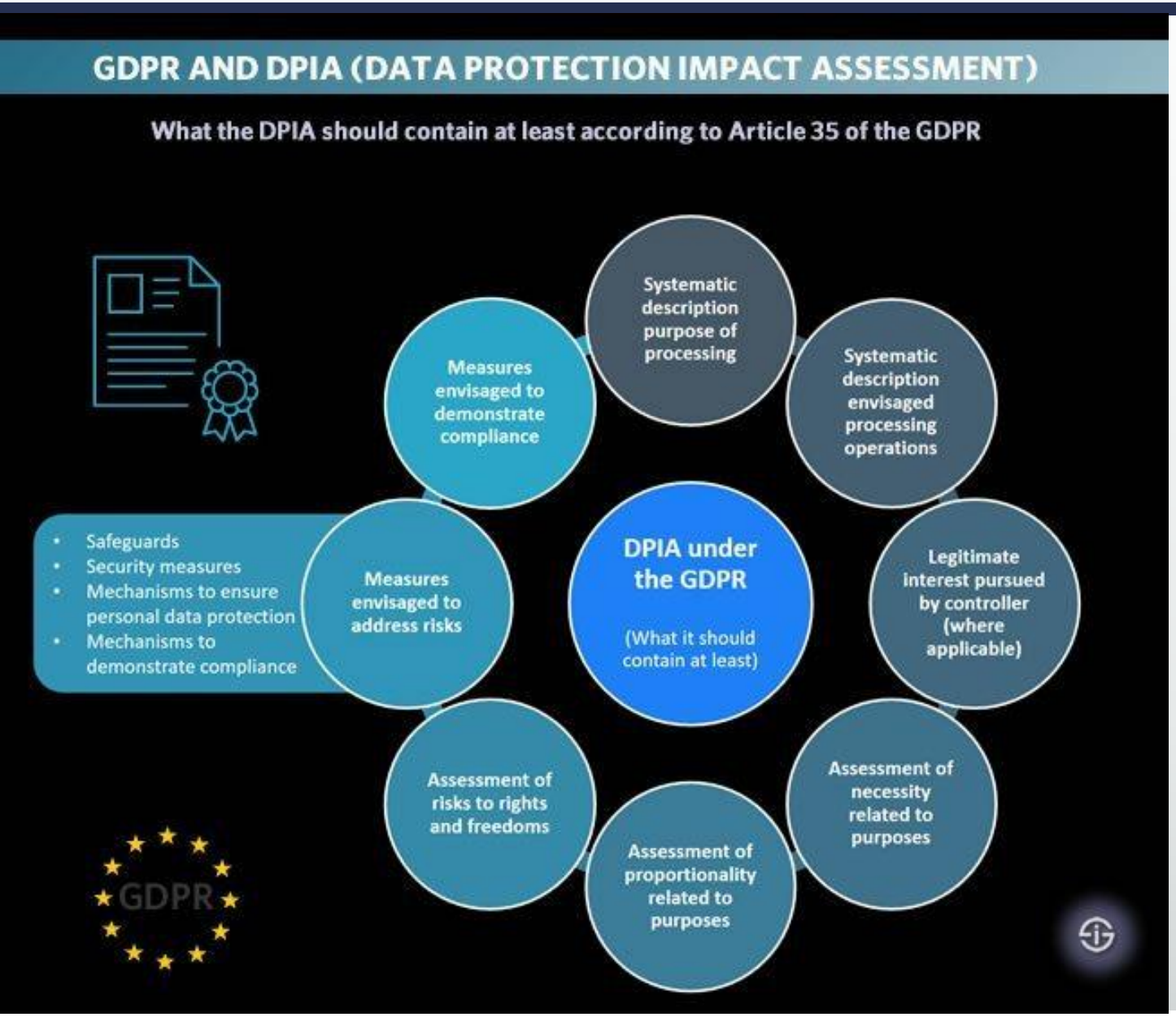
Named – each party relying on the consent needs to be clearly identified. The ICO's view is that 'even precisely defined categories of third party organisations' will not be sufficient.

Documented – organisations need to keep records showing what an individual was told, what they consented to and when and how consent was given.

Easy to withdraw – it must be as easy to withdraw consent as it is to give it. Individuals need to be told that they have the right to withdraw consent.

No imbalance – organisations cannot rely upon consent where there is an imbalance in the relationship so the individual doesn't have genuine choice.

Step 10: Data Protection Impact Assessment



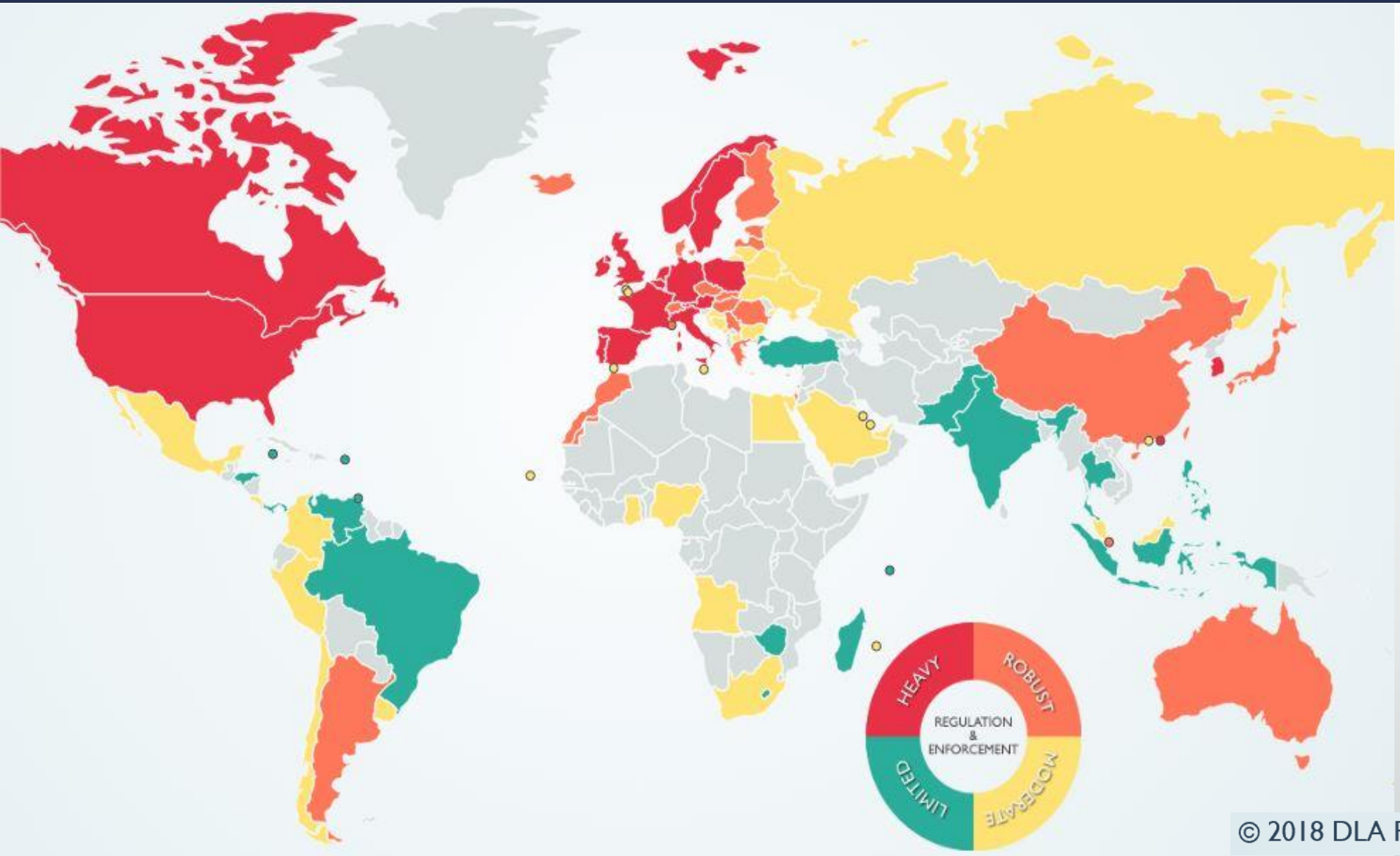
Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Step 11: Data Protection Officer

A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

STEALTHbits Technologies

Step 12: International



The GDPR contains relatively detailed rules on the conditions under which personal data may be transferred to third countries (or international organizations), as stated in the Preamble to the GDPR (101): "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation."

Initial reflections

- Realisation of the metadata problem – who controls metadata?
- How to share cyber security incident information involving private individuals' personally identifying data? (New regulatory environment starts to be discussed from September – renewal of NIS Directive, moving towards mandatory incident information sharing – cyber security invcident information may fall out of GDPR scope in the future.)
- There is no such thing as GDPR per sector, but there is NIST cybersercurity framework implementation difference among sectors – as different cyber security rules apply to a nuclear power plant and to a webshop selling flowers.
- Data stored in databases becomes problematic when the same data value becomes personally identifying data due to correlations – a taylor (non identifying) vs Mr. Taylor (personally identifying).

Art. 3 GDPR Territorial Scope

1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

1. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
2. the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Art. 3 GDPR Territorial Scope

GDPR Highlights

Territorial Scope

Scenario 1:

Processing personal data as an establishment of a data controller or a data processor in the EU, regardless of whether the processing takes place in the EU or not.

Scenario 2:

Any organisation which is not established in the EU but is processing personal data about data subjects who are in the EU

fileminders

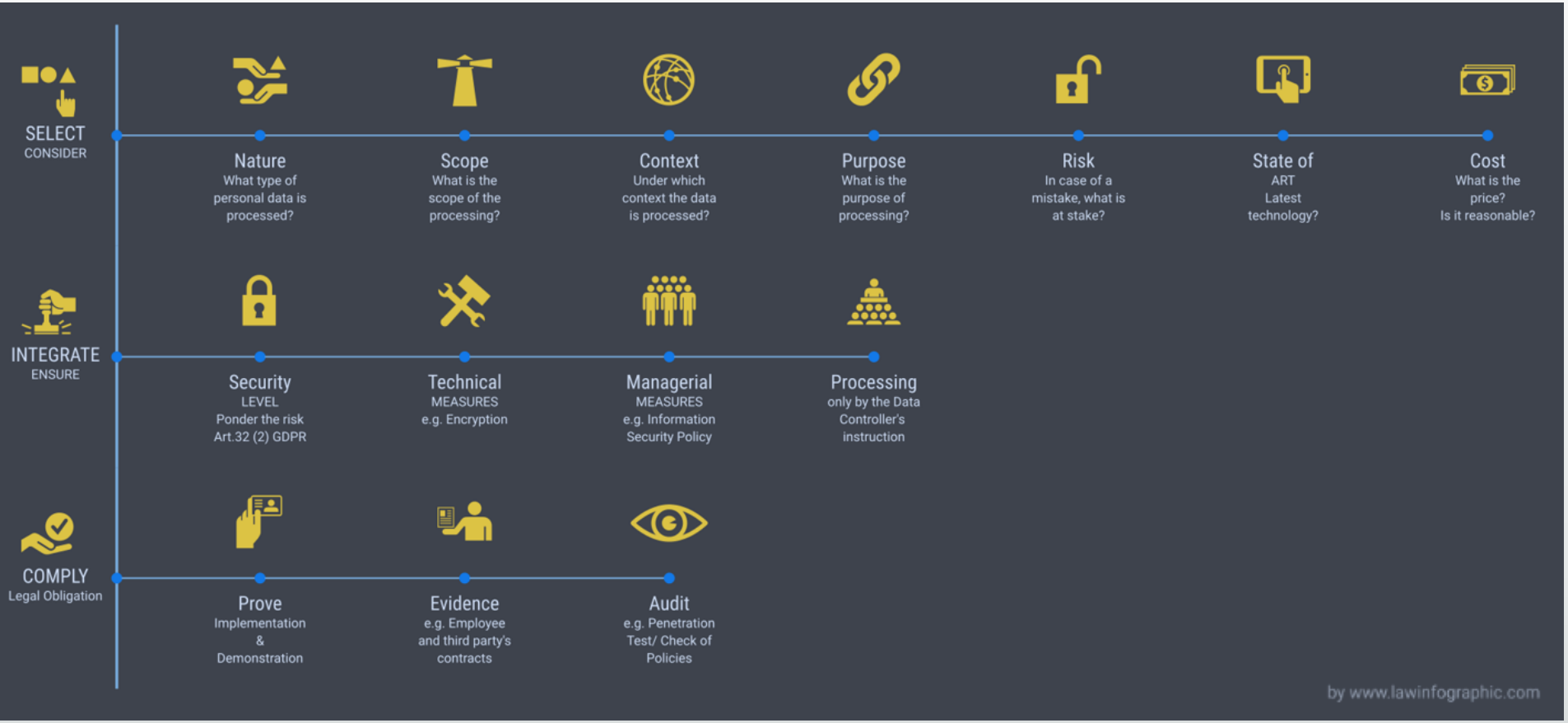
Art. 3 GDPR Territorial Scope

Art. 3 GDPR Territorial Scope – Conclusion

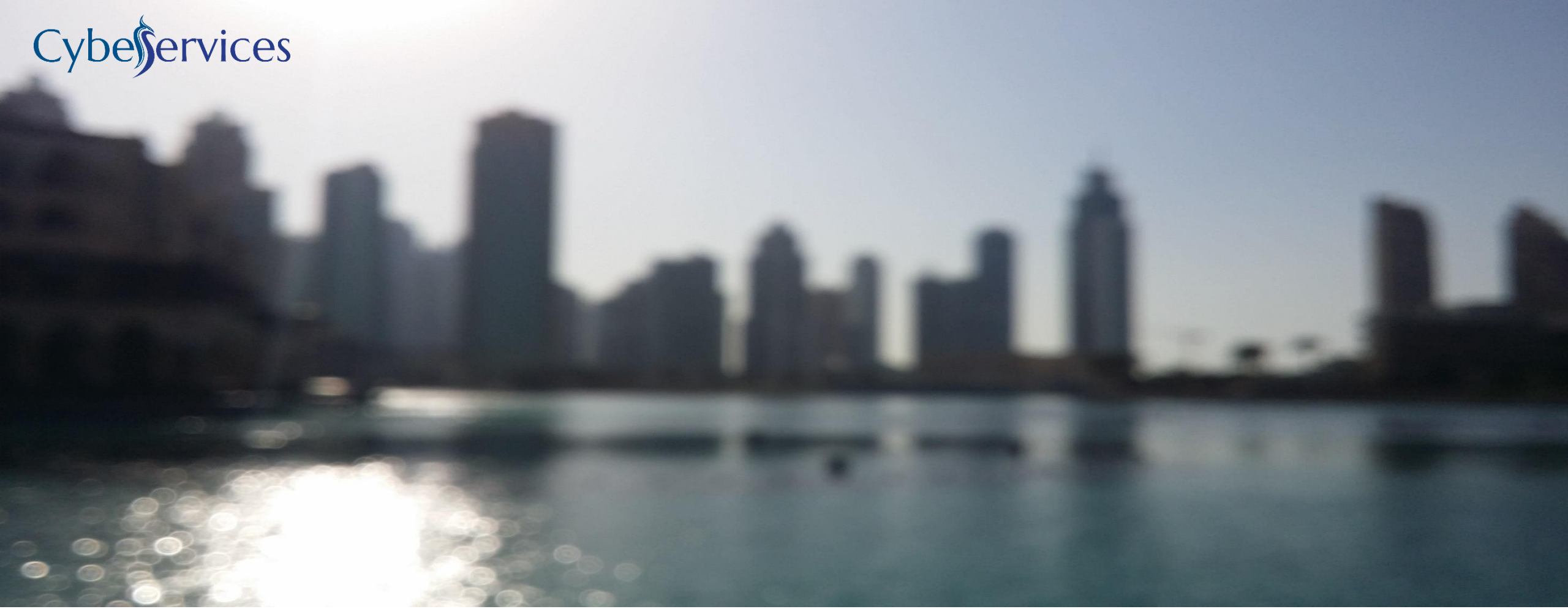
GDPR regulation applies to:

Regardless data controllers or processors are within the European Union or not, if data subjects are within the European Union physical (continental/geographycal) borders and use EU information infrastructure to interact.

Data Protection Solutions (– NIST Recommended)



To secure data from internal and external threats, article 32 of the GDPR, provides the following points to be considered in choosing a data protection solutions.

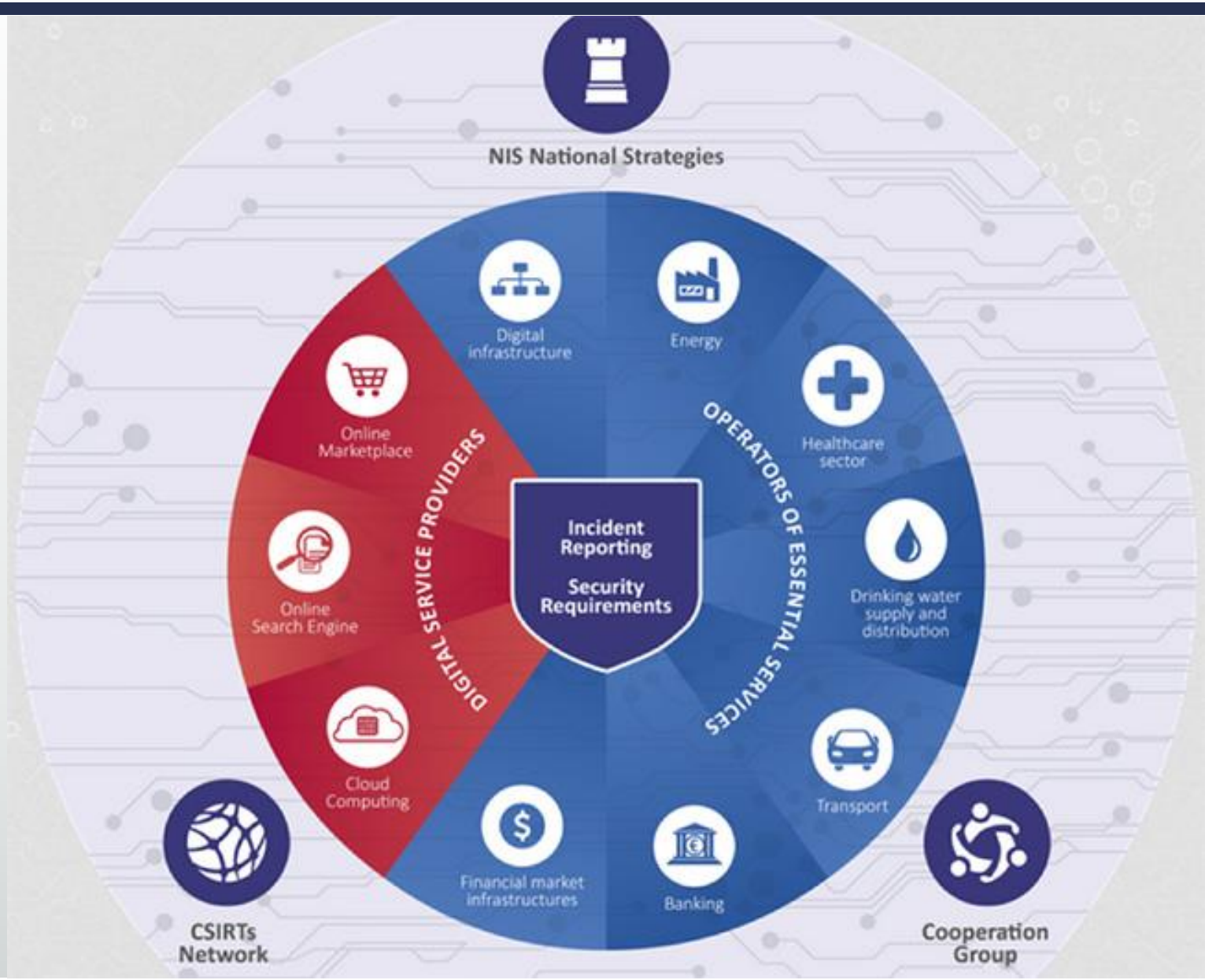


The EU Network and Information Security Directive – To Help Implement GDPR

Scope

The new EU NIS directive will set out cybersecurity obligations for **operators of essential services and digital service providers**. These operators will be required to take measures to manage cyber risks and report major security incidents. And, the e-commerce platforms, search engines and cloud services will be covered by the scope of the directive.

The modification process has begun according schedule to NIS. The national Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT) will be selected and will be converted according to the incident notification policy.



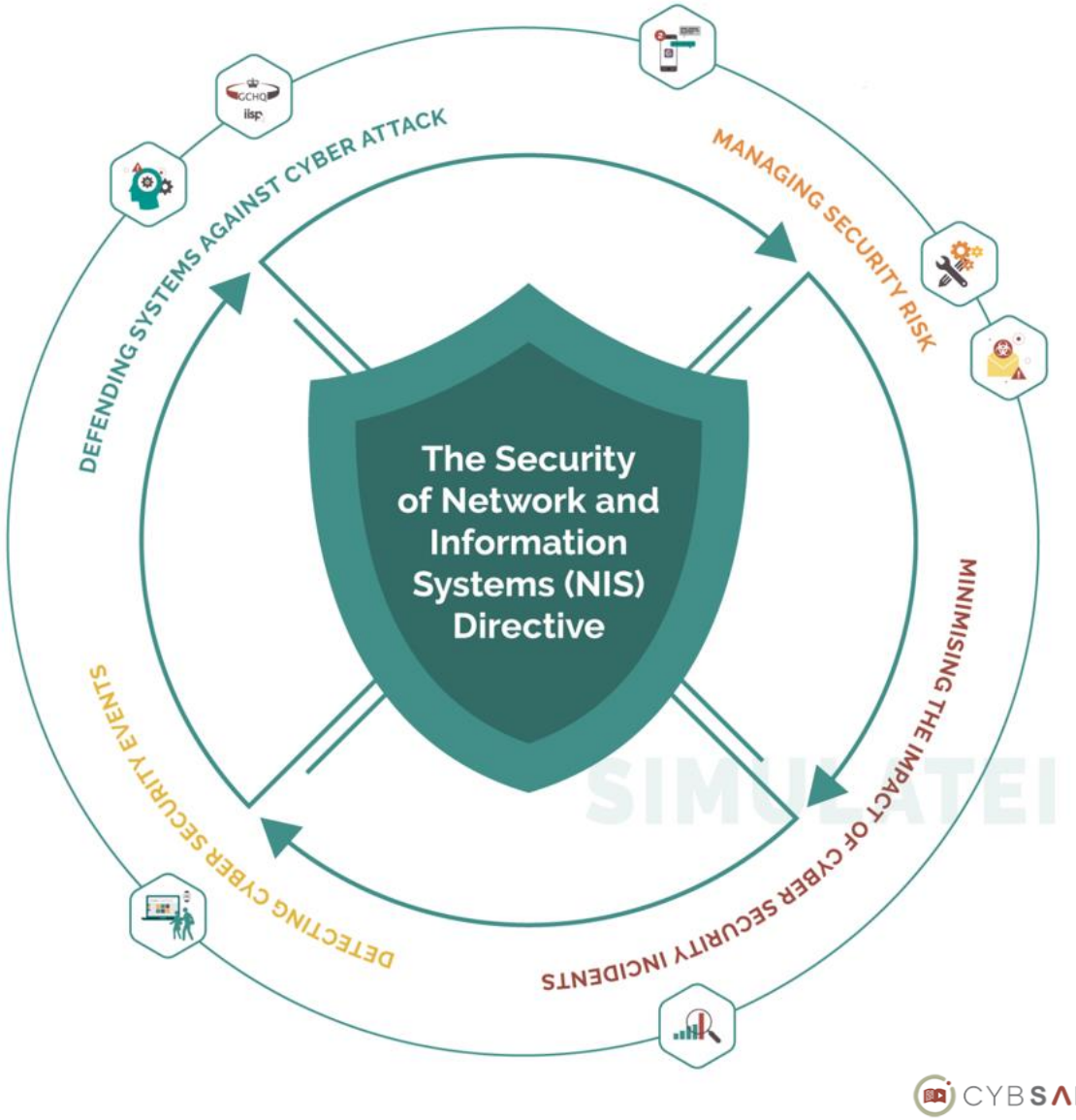
Principles

Defending systems against cyber attack

Advanced proprietary and staff attitude surveys are used to measure and report om what an employee knows, how they act and what they think when considering cyber security. This allows organisations to visualise, report an and reduce human risk, evaluate effectiveness, evidence behaviour change and progressively develop organization culture.

Detecting cyber security events

Employees are encouraged to actively contribute to security by offering advice on organizational policies and processes, reporting suspicious activity, and to provide POV insights into the way they work.

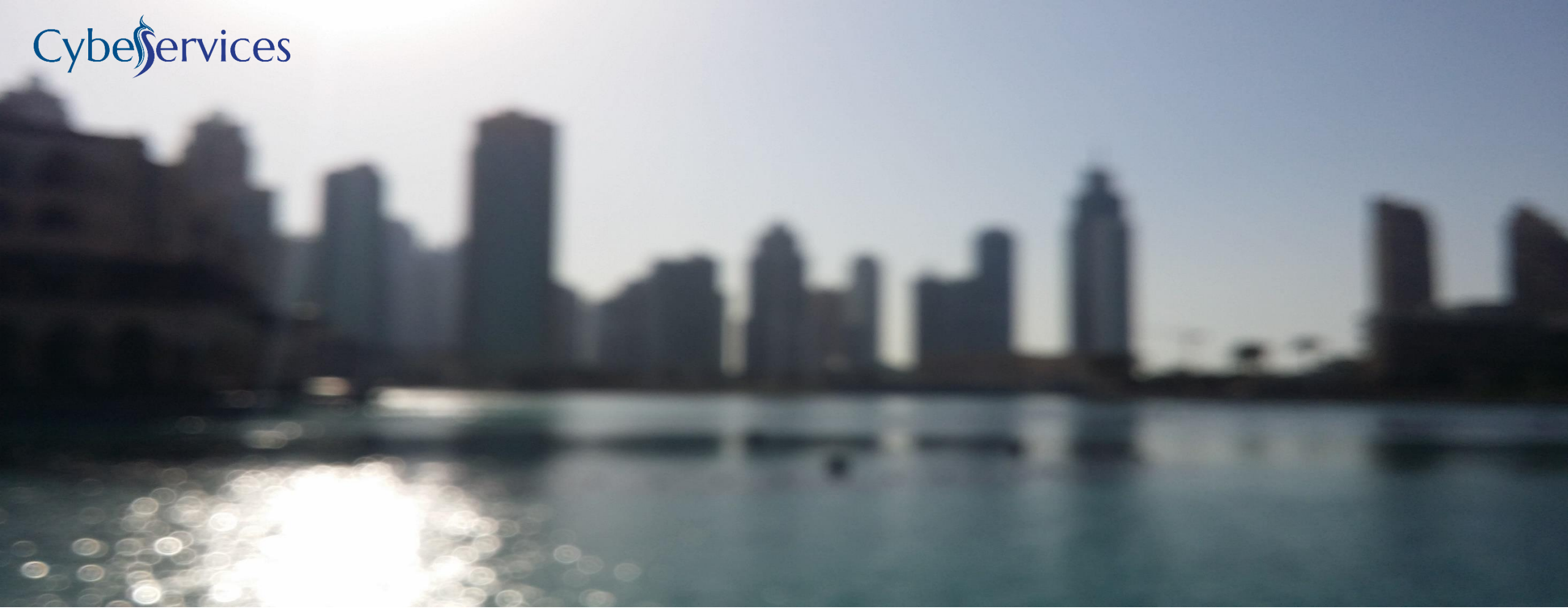


Managing security risk

Need to be training and guidance on the threat landscape, adversarial thinking and allows organization to assess the security posture of their supply chain with its supply chain assurance tool. Human behaviour and its implication on risk is regularly tested through simulated attack including phishing, smishing and USB drops.

Minimising the impact of cyber security incidents

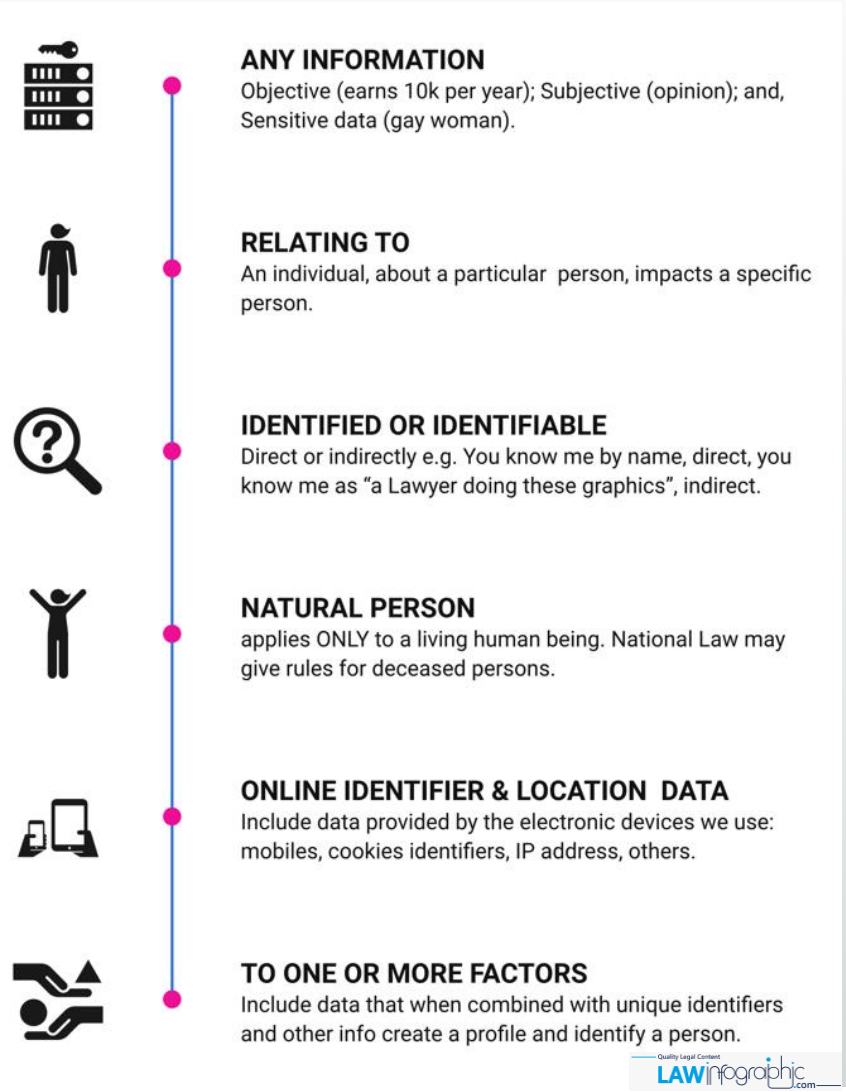
Make use of behavioural science principles to provide essential guidance to employees so that they understand the importance of, and are able to support, business continuity and disaster recovery responses.



The GDPR and NIST

GDPR + NIST Personal Data and Data Classification

GDPR Data classification



NIST – Risk matrix

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modi-fication or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Cyber Services Best Practice GDPR Compliance – 3rd Step NIST

1. **Legal compliance**: regulatory instruments (legislation, internal regulations, etc.) fully comply with GDPR requirements.
2. **Standard compliance:** the organization's operations/services/products has been standard solutions that fosters GDPR compliance.
3. **GDPR-NIST compliance:** the organization's services/products have been NIST 800-53 certification.
4. **Vulnerability investigation:** the organization's services and products are ripe for complex cyber security testing.

NIST Documents

The **Cybersecurity Framework** consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework is prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

The **NIST 800-53 appendix J** provides a structured set of **data protection** controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing **privacy controls** concerning the entire life cycle of personally identifiable information, whether in paper or electronic form. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security.
Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of personally identifiable information.

The **NIST 800-53 appendix D** contains the **security control baselines** that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems.

GDPR and NIST Mapping: Documentations and Keys

Documentation background	GDPR	NIST 800-53 Rev4 Appendix J - Privacy Control Catalog: Privacy Controls, Enhancements, and Supplemental Guidance	NIST Cybersecurity Framework	NIST 800-53 Rev4 Appendix D - Security Control Baselines : Low-Impact, Moderate-Impact, and High-Impact Information Systems

	Chapter/Article	Title	Paragraph	Text	Referenced by	Requirement subject	Citation	Requirement ID	Requirement	Alternative	Prioritization
Key to CS document columns' header	No. Of chapter, section or article of the GDPR regulation	Title Of chapter, section or article of the GDPR regulation (literally included)	No. Of paragraphs within the articles of the GDPR regulation (if any)	Text of the of the paragraph or of the including article in the GDPR regualtion (literally included)	List of additional articles referring to the given article	Subject of the requirements, who is responsible for complying with those requirements. Only requirements in respect of data owners and data managers are processed here. Where the cell is empty both rules are concerned, given that the requirement can be interpreted here.	Unit (point) within the article or in the paragraph related to the requirement.	Uniqe identification of the requirement, which can be referred to. Formula: K-<no. Of article>-<no. Of paragraph>-<running serial number> If no paragraph then the number is 0.	Explicit criteria included in the article, which compliance is searched here. One article or paragraph can generate more requirements. Wording of the requirements are following strictly the text of the regulation, so that it can be analyzed in their own context, even without reading the complete regualtion.	If the compliance is provided in case of alternative fulfillment of a requirement, then the ID of the alternative requirement is listed here.	Governing emphasis of meeting the article's requirement, defined on the basis of the possible penalty imposed or risk occured.

	NIST PRIVACY CONTROL CATEGORY	NIST PRIVACY CONTROL
Key to CS document columns' header	ID of the NIST personal data protection control catalog supporting the fullfillment of the requirements.	ID of the NIST personal data protection control cataloges supporting the fullfillment of the requirements. The personal data protection controls are defined in the NIST 800-53 Recommendation Appendix "J".

	CSF Function+Cat	CSF Subcategory
Key to CS document columns' header	ID of NIST cybersecurity framework functions and the including control cataloges supporting the fulfillment of the requirements.	ID of subcatalog controls defined by the NIST cybersecurity framework supporting the fulfillment of the requirements. NIST cybersecurity framework functions, control catalogs and subcatalogs are defined by the NIST „Framework for Improving Critical Infrastructure Cybersecurity" recommendation.

	NIST CYBERSEC CONTROL CATEGORY	NIST CYBERSEC CONTROL
Key to CS document columns' header	ID of NIST data protection catalogs under the subcatalogs defined by the NIST cybersecurity framework supporting the fulfillment of the requirements.	ID of NIST data protection catalogs under the control subcatalogs defined by the NIST cybersecurity framework supporting the fulfillment of the requirements. The cybersecurity controls and catalogs are defined by NIST 800-53 recommendation.

GDPR and NIST Mapping: MS Office 365

	NIST CYBERSEC CONTROL CATEGORY			NIST CYBERSEC CONTROL	Comment	Fines: 20M € or	Fines: 10M € or 2%	
Examples from the Cyber Services document	All, PM, PS			*-1, PM-1, PS-7			x	
Header of Office 365 audit document acc. To the NIST 800-53A (Rev. 4)	**Control Family Id**	**Control Family Name**	**Control Family Description**	**Control Id**	**Control Title**	**Office 365 Control Ids**	**Implementation Details**	**Testing Details**
Example from the MS audit document	PS	Office 365 Personnel Security Control Family	Understand how Microsoft addresses personnel security for Office 365, including policies and procedures, personnel screening, termination, transfer, and sanctions, access agreements, and third-party personnel security.	PS-07(a)	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers.	PS-0131	In all of its contracts, Microsoft establishes screening requirements for third-party providers to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. Any third-party personnel with access to Office 365 must pass the same personnel screening process for the requirements established for the risk categorization of their role.	Examined the Microsoft Office 365 Multitenant System Security Plan Version 3.01, dated May 13, 2016 and determined that Microsoft establishes screening requirements for third-party providers to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. Any third-party personnel with access to Office 365 must pass the same personnel screening process for the requirements established for the risk categorization of their role.

+

NIST PRIVACY CONTROL CATEGORY	NIST PRIVACY CONTROL
AR, DM, IP, TR	AR-1, AR-3, DM-2, IP-2, IP-3, IP-4, TR-1

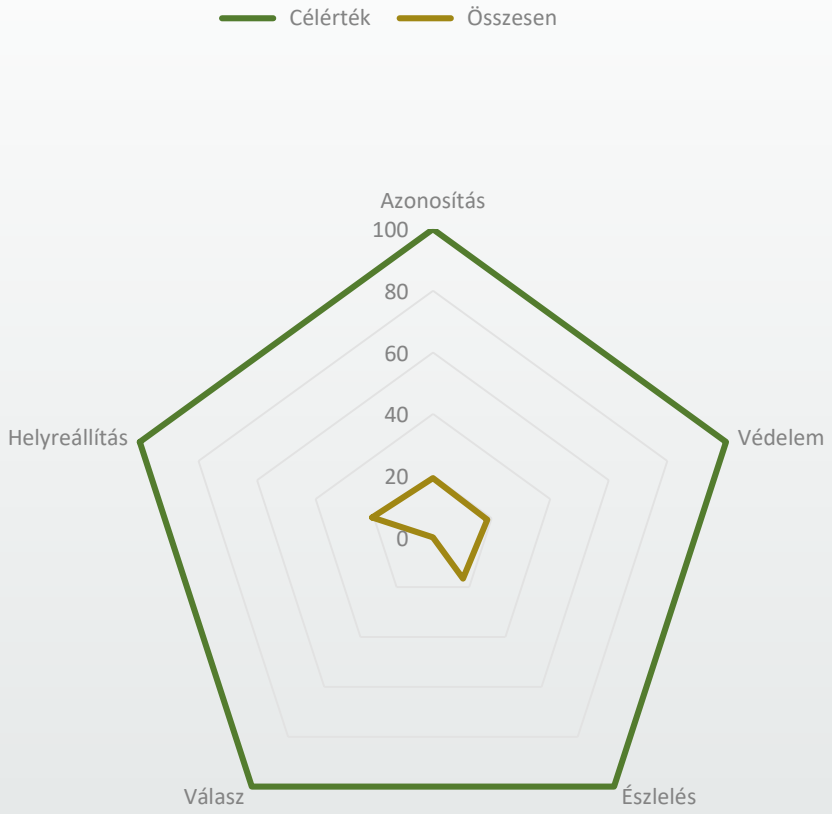
+

CSF Function+Cat	CSF Subcategory
ID	ID.GV-1, ID.GV-2, ID.GV-3

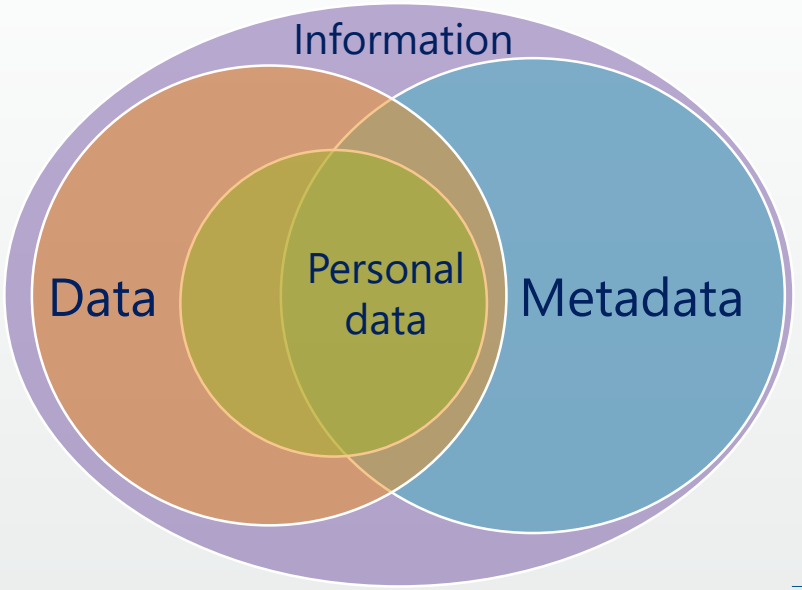
=

	Chapter/Article	Title	Paragraph	Text	Requirement	Prioritization
Examples from the Cyber Services document	Article 28	Data Processor	(3)	Data management carried out by the data processor based on Union or Member State law ..	The data processor taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	High

A NIST GAP Analysis Result



Data and Information: Definitions



Information is any entity or form that provides the answer to a question of some kind or resolves uncertainty.

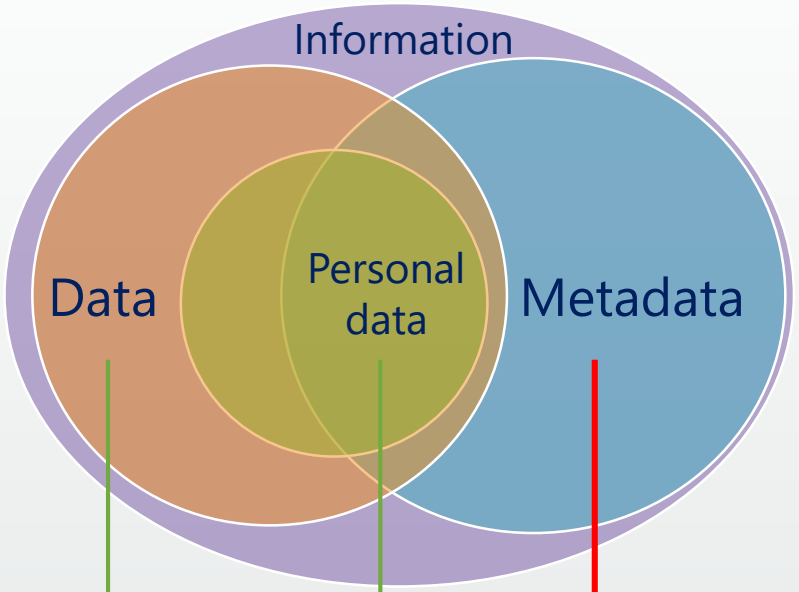
Data is a set of values of qualitative or quantitative variables.

Personal data means any information relating to an identified or identifiable natural person an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Metadata means "data about data". Metadata is defined as the data providing information about one or more aspects of the data; it is used to summarize basic information about data which can make tracking and working with specific data easier.
Some examples include:

- Means of creation of the data;
- Purpose of the data;
- Time and date of creation;
- Creator or author of the data;
- Location on a computer network where the data was created;
- Standards used;
- File size;
- Data quality;
- Source of the data;
- Process used to create the data etc.

Future: Legislation Harmonisation

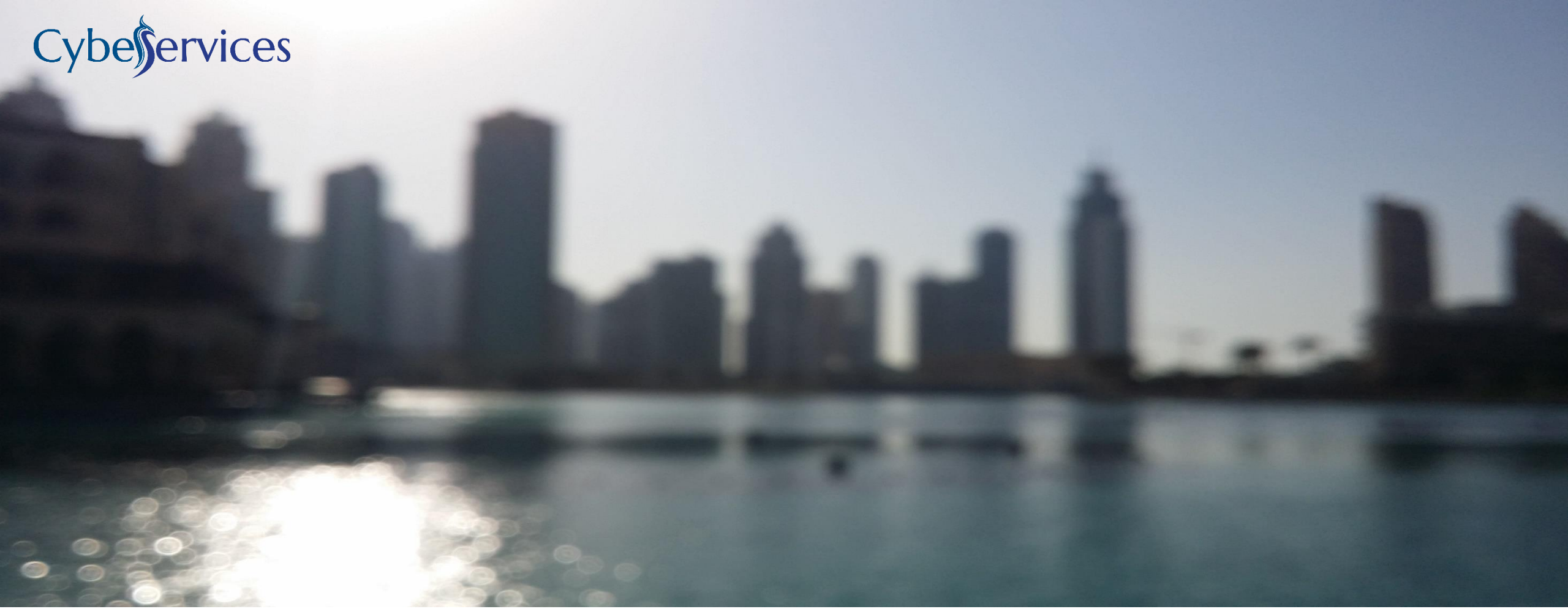


Is this a **data protection** incident (GDPR)?

Is this an **information security** incident (NIS)?

What data was corrupted?
Where are these data?
Which database/electronic information system contains these data?
What other database/electronic information system have compromised?
What other data are in danger?
Do I know where to report this and what?

Data about data → I don't KNOW → The possible future: legal harmonisation



Thank you

www.cyber.services