



ICTLC

Legal cybersecurity landscape: how to create an effective and integrated privacy and cybersecurity compliance framework

Prof. Dr. Paolo Balboni - Founding Partner ICTLC

Professor of Privacy, Cybersecurity, and IT Contract Law at
the European Centre for Privacy & Cybersecurity at Maastricht University
E: paolo.balboni@ictlegalconsulting.com / Twitter: @balbonipaolo

Helaine Leggat - Managing Partner - ICTLC Australia

Attorney at Law, CISSP, CISM, CIPP, CIPT, GAICD
E: helaine.leggat@ictlegalconsulting.com / Twitter: @helaineleggat

Francesco Capparelli - Chief Cyber Security Advisor ICTLC

Chief Cyber Security Advisor ICT Cyber Consulting - Senior
E: francesco.capparelli@ictcyberconsulting.com / Twitter: @FraKrelli

Milan - Bologna - Rome - Amsterdam - Melbourne - Madrid - Helsinki

Agenda

1. Cyber stats & the cost of a data breach
2. Privacy and Cybersecurity European and Australian Legal Framework
3. Major sanctions in the EU
4. Methodology to create an integrated privacy and cybersecurity compliance framework
5. Quantifying privacy ROI & cybersecurity ROSI
6. Conclusions & recommendations

A large, stylized graphic of an open padlock, rendered in a golden-brown wireframe or mesh style. The padlock is open, with the shackle at the top and the body at the bottom. The text 'Cyber stats & the cost of a data breach' is superimposed over the center of the padlock.

Cyber stats & the cost of a data breach

Cybersecurity outlook

- Covid 19: Not just a health crisis, but also a cyber crisis.
- Rapid move to remote work and to appropriate tools.
 - According to CISCO: 41% of organizations were prepared from a privacy and security perspective and “87% of individuals expressed concern with the privacy protections involved in the tools they needed to work and interact remotely.”
- Need for increased data sharing.

Cisco 2021 Forged by the Pandemic: The Age of Privacy Data Privacy Benchmark Study
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf

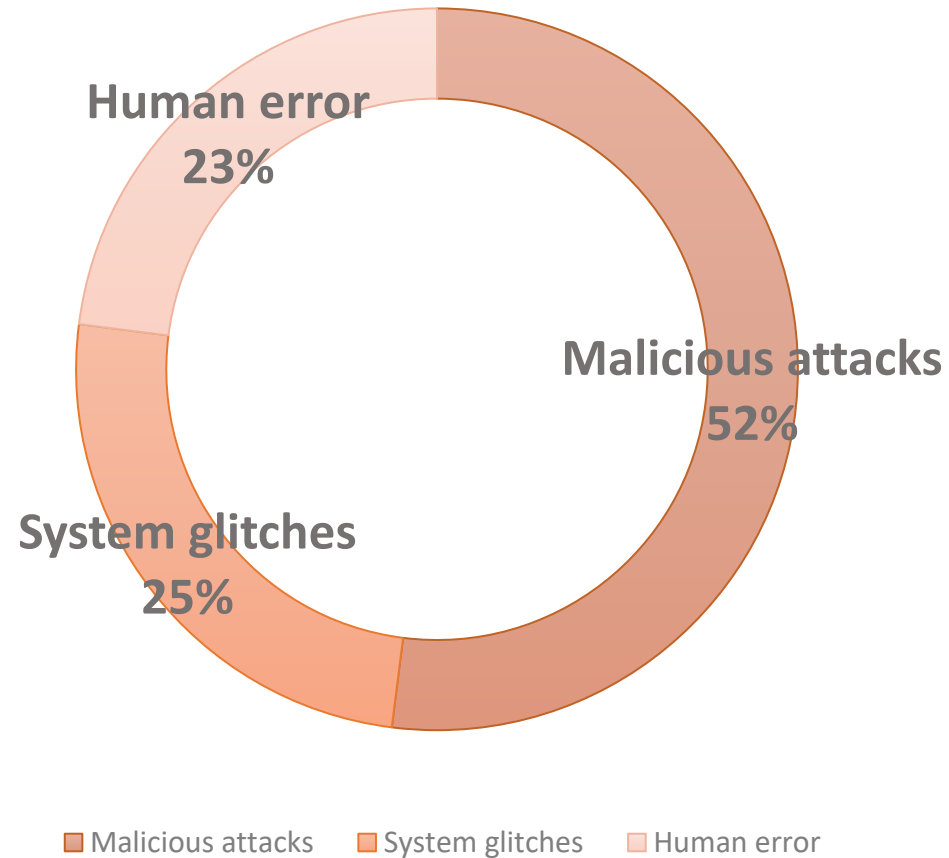
Threat landscape

“During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.”

- ENISA Threat Landscape



Cause of Data Breaches



“Cost of Data Breach Report.” 2020. IBM Security, Ponemon Institut
<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>

Main incidents

84%_ of cyberattacks rely on social engineering

67%_ of malware was delivered via encrypted HTTPS connections³⁴

230.000_ new strains of malware every day

6_ months in average is what it takes to detect a data breach

71%_ of organizations experienced malware activity that spread from one employee to another³⁵

Digital Services_ Services such as e-mail, social and collaborative platforms and cloud providers were under attack during 2019. These were also used as proxies for further attacks.

Government Administration_ The financial returns from ransoms paid makes the public sector one of the most attractive targets for ransomware attacks.

Technology Industry_ The technology industry was under attack in 2019 mainly through supply chain attacks trying to compromise the development of software through zero-day exploits and backdoors attacks.

Financial_ The number of incidents with financial organisations and not necessarily banks, increased substantially during the reporting period.

Healthcare_ The number of attacks against the healthcare sector continues to grow.

Main incidents in the EU and worldwide ENISA Threat Landscape
<https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>

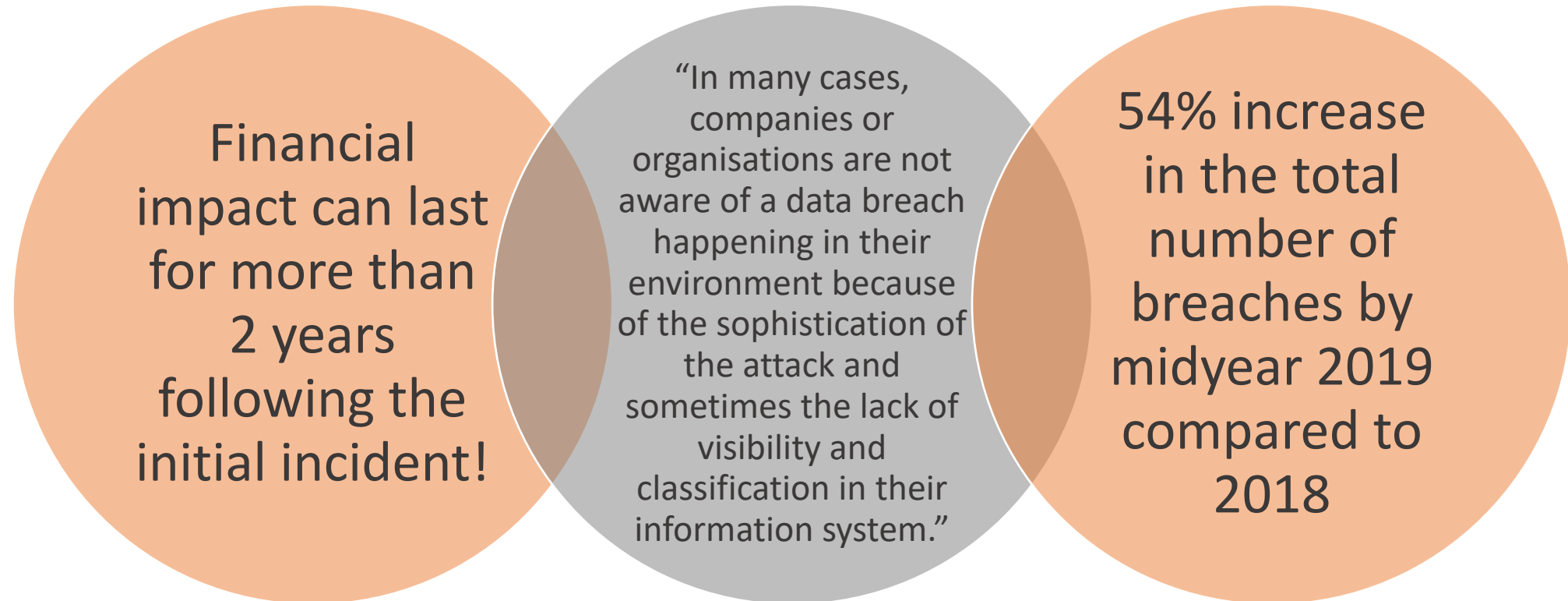


Top 15 cyberthreats (ENISA)

1. Malware
2. Web-based Attacks
3. Phishing
4. Web Application Attacks
5. SPAM
6. Distributed Denial of Service (DDoS)
7. Identity Theft
8. Data Breach
9. Insider Threat
10. Botnets
11. Physical Manipulation, Damage, Theft and Loss
12. Information Leakage
13. Ransomware
14. Cyber Espionage
15. Cryptojacking

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>

Data Breaches on the rise



From January 2019 to April 2020: Data breach ENISA Threat Landscape
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach>

Cost of Data Breaches

Cost for enterprises or large organisations (more than 25.000 employees) = ca. **€173 per employee**

Cost for small companies (500-1.000 employees) = ca. **€3.000 per employee**

From January 2019 to April 2020: Data breach ENISA Threat Landscape <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach> and “Cost of Data Breach Report.” 2019. IBM Security, Ponemon Institut <https://www.ibm.com/security/data-breach>



Privacy and Cybersecurity European and Australian Legal Framework

Europe: Key GDPR security provisions

Art. 5.1.f: Personal data shall be: (...) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*'integrity and confidentiality'*).



Art. 32 *Security of processing*: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (...)



Art. 33 *Notification of a personal data breach to the supervisory authority* and Art. 34 *Communication of a personal data breach to the data subject*



Art. 28 *Processor*: Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law (...). That contract or other legal act shall stipulate, in particular, that the processor: (...) takes all measures required pursuant to Article 32.

European Cybersecurity Strategy

The new EU Cybersecurity Strategy was adopted on 16 December 2020 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy.

The Strategy mainly:

- ✓ covers the security of essential services such as hospitals, energy grids and railways;
- ✓ addresses the security of the ever-increasing number of connected objects in our homes, offices and factories;
- ✓ focuses on building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace; and
- ✓ outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to the EU and Member States.

European Commission, The Cybersecurity Strategy, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

European Cybersecurity Legislation, Authority and Certification -> NIS (and NIS2)

Directive on security of network and information systems - **NIS Directive**

Compliance with the NIS Directive seeks to enhance overall cybersecurity through putting in place the legal and organizational measures within the Member States for that effect

Now implemented in all countries, it was reviewed at the end of 2020 and the proposal for a Directive on measures for a high common level of cybersecurity across the Union **NIS2 Directive** was presented by the Commission on 16 December 2020

European Cybersecurity Legislation, Authority and Certification → ENISA



- ENISA, the ‘European Union Agency for Network and Information Security’, is the EU agency that deals with cybersecurity.
- It provides support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

EU: Cybersecurity Legislation, Authority and Certification → Cybersecurity Act

- The Cybersecurity Act strengthens the role of ENISA.
- The agency now has a permanent mandate and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU.
- It also has more financial and human resources than before.
- The EU Cybersecurity Act introduces a **Europe-wide cybersecurity certification framework for ICT products, services and processes**:
 - ENISA Cybersecurity Certification: Candidate EUCC Scheme V1.1.1.
- Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union.



The EU Cybersecurity Act, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

Australian Commonwealth & New South Wales privacy regulatory framework

Laws: Privacy, Personal Information (PI), Data Subject and Mandatory Breach Notification

Act	Regulator	Comments
Commonwealth		
Privacy Act 1988 (Cth)	Office of the Australian Privacy Commissioner (OAIC) <ul style="list-style-type: none"> Privacy FOI Consumer Data Right Safeguards (CDR) (& health)	Applies to Australian Commonwealth agencies, large businesses (revenue over \$3 million pa), health service providers, some small businesses and non-government organisations, but not to state government agencies or local councils. Excludes "Employee Records". 13 Australian Privacy Principles (APPs) <ul style="list-style-type: none"> APP 8 - cross-border disclosure of personal information APP 11 - security of personal information <ul style="list-style-type: none"> MDB report to OAIC for "Eligible Data Breach" Report when "reasonably practicable" 30-day assessment for suspected breach
Spam Act 2003 (Cth)	Australian Communications and Media Authority (ACMA)	Applies to marketing emails or messages (text)
Do-Not-Call Register	ACMA	Applies to unsolicited telemarketing calls. Consumer home, mobile or fax numbers
New South Wales		
Privacy and Personal Information Protection Amendment Bill (2020)	Information and Privacy Commission NSW	Will apply the to all state-owned corporations that are not regulated by the Commonwealth Privacy Act 1988 Mirrors the Privacy Act 1988 (Cth) NDB

Australian privacy regulatory framework States and Territories

Laws: Privacy, Personal Information (PI), “Data Subject”

States and Territories

	Act	Regulator
Victoria	Privacy and Data Protection Act 2014 (Vic)	Office of the Victorian Information Commissioner (OVIC)
	Health Records Act 2001 (Vic)	Office of the Health Commissioner (OHC) administers consumers and health care provider complaints
New South Wales	Privacy and Personal Information Protection Act 1998 (NSW)	NSW Information and Privacy Commission (NSWIC)
	Health Records and Information Privacy Act 2002 (NSW)	NSWIC
Queensland	Information Privacy Act 2009 (Qld) (IPA)	Queensland Office of the Information Commissioner. Covers the Qld public sector. Qld Health Ombudsman receives health service complaints
Tasmania	Personal Information and Protection Act 2004 (Tas)	Tasmanian Ombudsman accepts complaints
South Australia	-	SA Privacy Committee handles privacy complaints related to state government agencies’ compliance with a set of Information Privacy Principles
Western Australia	-	Office of the Information Commissioner (OICWA) administers some aspects of FOI. Health and Disability Services handles health and disability
Northern Territory	Information Act 2002 (NT) (IA)	Office of the Information Commissioner Northern Territory (OICNT) oversees the privacy provisions of the IA
Australian Capital Territory	Information Privacy Act 2014 (ACT) (IPA)	Information Privacy Commissioner under the IPA regulates ACT public sector agency PI. OAIC handles some functions of the ACT Information Privacy

Australian surveillance regulatory framework

Laws: Telecommunications interception and surveillance

Commonwealth	Ministerial Portfolio	Comments
Telecommunications (Interception and Access) Act 1979 (TIA)	Department of Home Affairs	Carriers and carriage service providers to have capability to intercept a communication passing over their system in accordance with a warrant.
Surveillance Devices Act 2004 (SDA)	Department of Home Affairs	An eligible agency can apply for a warrant to use a surveillance device to investigate a relevant offence (for AFP).
Telecommunications Act 1997 (TA)	Department of Communications and the Arts	Imposes obligations on telecommunications industry participants, including to provide assistance to officers and authorities of the Commonwealth, states and territories reasonably necessary for law enforcement and national security.
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)	Department of Home Affairs	Assistance to law enforcement and intelligence on metadata and stored communications: SMS, email, voicemail, and to intercept comms with warrants. Allows phone calls to be tapped. A technical assistance request asks the provider to do “acts or things” to ensure the provider is capable of giving certain types of help to the Australian Secret Intelligence Organisation, Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency.
Pending Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020	Department of Home Affairs	To introduce: Data disruption warrants to enable the Australian Federal Police and Australian Criminal Intelligence Commission to disrupt data by modifying, adding, copying or deleting data to frustrate offences online and make “minor technical corrections” ; network activity warrants to collect intelligence by permitting access to the devices and networks ; takeover warrants to enable access to a person's online account to gather evidence; and ... 10 Acts to make consequential amendments.
Pending Clarifying Lawful Overseas Use of Data Act (CLOUD)	Department of Home Affairs	Australia is likely to be the next qualifying foreign government (after the UK) to enter into an agreement with the United States under its Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The Act creates a legal framework regulating how law enforcement can access data across borders .

****Data Surveillance:** Surveillance Devices Acts for states and territories provide privacy protection by creating offences for the unauthorised use of listening devices, optical surveillance devices, tracking devices, and data surveillance devices.*

Australia: surveillance implications

TRANSBORDER DATA FLOW - EU & US

European Commission to release revamped SCCs June 4 2021

Reynders said companies could seek to **protect personal data from being accessed by governments in third countries** by encrypting the data or processing it in a way that it cannot be attributed to a specific individual without the use of additional details.

Companies that export personal data outside the European Economic Area **must assess the surveillance laws and practice of intelligence agencies of the third country** that may impede the effectiveness of the standard contractual clauses and, if such impediments exist, must implement supplementary measures.

Justice Commissioner Didier Reynders said the European Commission will adopt revamped standard contractual clauses (SCCs).

"We have incorporated some elements of transparency (and) accountability in full compliance with the (EU General Data Protection Regulation)"



Standards and security (examples only)

Commonwealth	Victoria	Industry Sector - Finsec
Protective Security Policy Framework (PSPF) Australian Government entities to implement policy across: <ul style="list-style-type: none"> • Security governance • Information security • Personnel security • Physical security 	Victorian Protective Data Security Standards (VPDSS) 12 high level mandatory requirements to protect public sector information across all security areas including: <ul style="list-style-type: none"> • Governance • Information security • Personnel security • ICT security • Physical security 	APRA Standards: <ul style="list-style-type: none"> • CPS 234 - Information Security • CPS 220 - Risk Management • CPS 235 - Managing Data Risk • CPS 231 - Outsourcing Guides: <ul style="list-style-type: none"> • CPG 234 - Management of Security Risk in Information Technology • CPG 220 - Risk Management • CPG 235 - Managing Data Risk • CPG 231 - Outsourcing ASIC <ul style="list-style-type: none"> • Report 468 - Cyber Resilience Assessment • Report 429 - Cyber Resilience Health Check • CP 314 - Market Integrity Rules for Technological Integrity and Operational Resilience

**Examples only: This slide excludes other States and Territory requirements.*

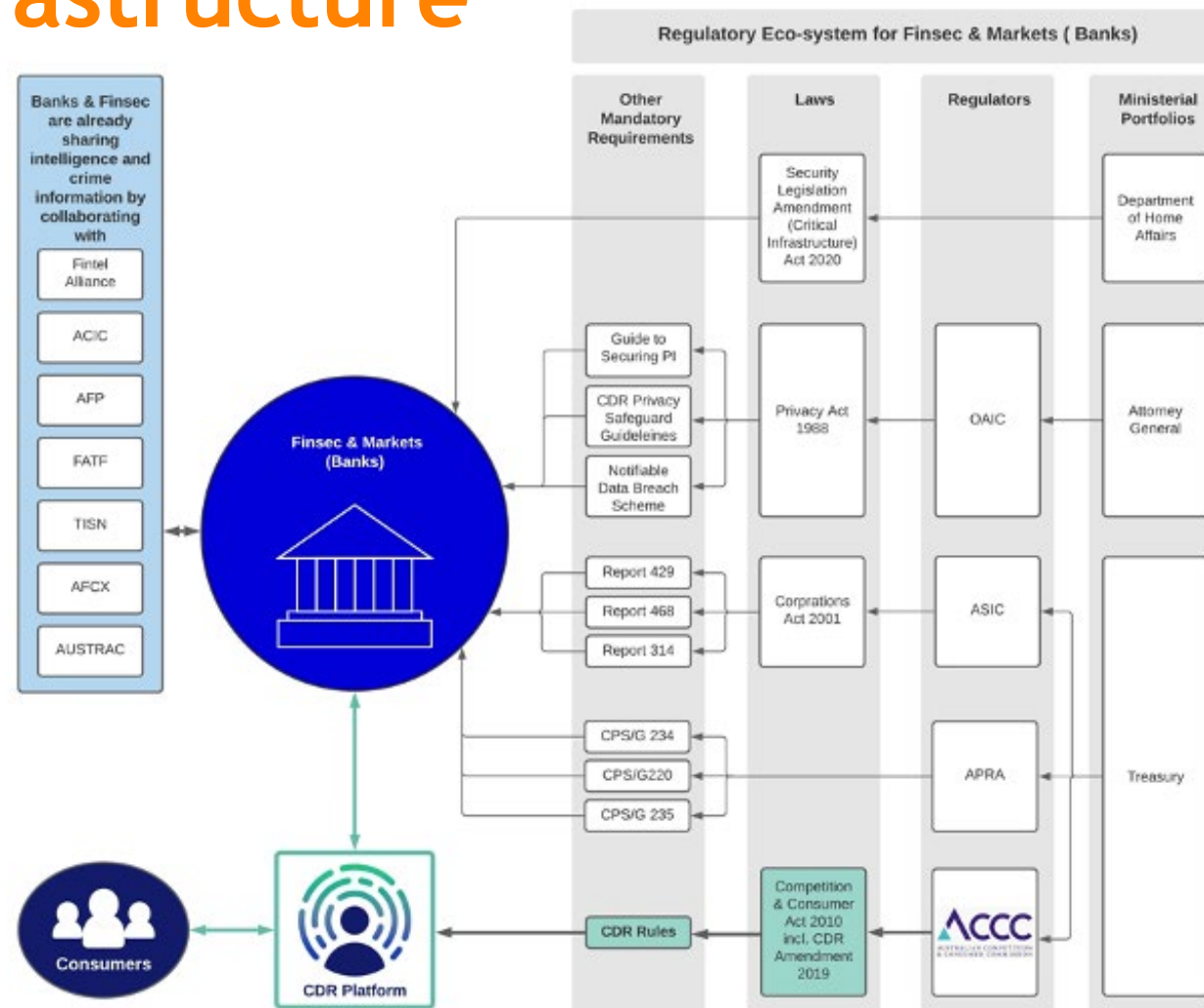
Privacy & corporate sector regulators CDR and Critical Infrastructure

EU Commission NIS 1 and 2. Australian 'equivalent effect':

Security of Critical Infrastructure Act 2018 (Cth) covers specific entities in electricity, gas, water and ports sectors.

Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth), covers:

- communications
- financial services and markets
- data storage or processing
- the defence industry
- higher education and research
- energy
- food and grocery
- health care and medical
- space technology
- transport
- water and sewerage



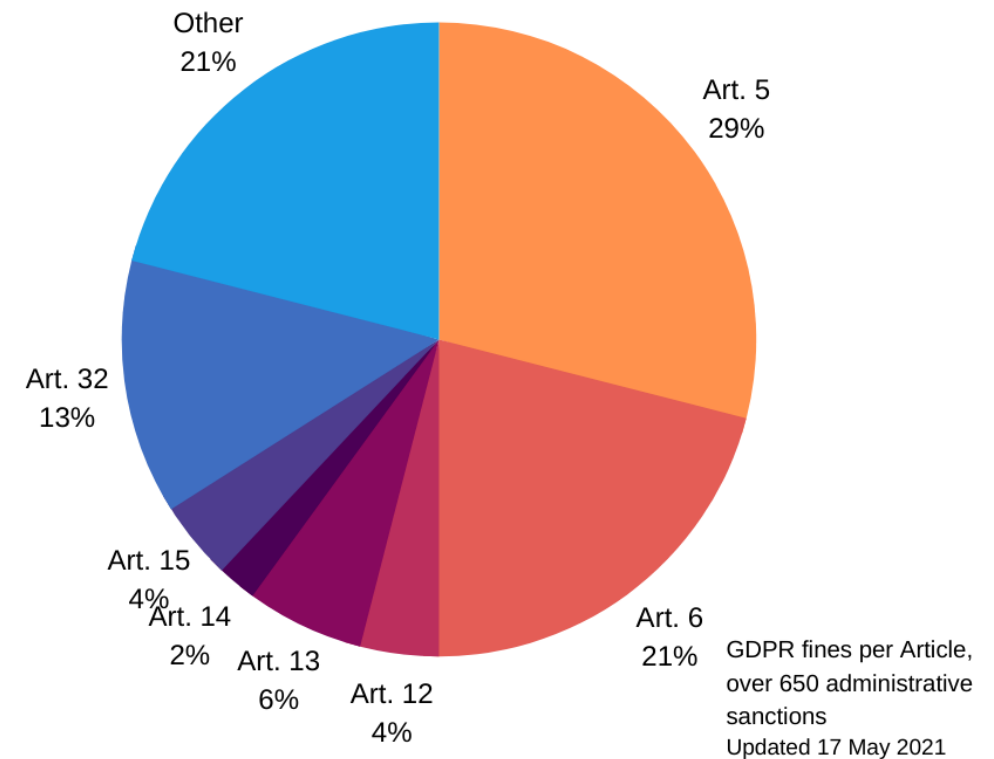
The background of the slide is a photograph of the United States Supreme Court building, showing its iconic portico with six large columns and a pediment with sculptures. The image has a warm, orange-toned filter applied to it.

Major sanctions in the EU

Focus on Data Security

Based on the analysis of more than 650 enforcement actions, the majority of administrative fines to date (*some of which are combined, e.g., violation of Arts. 6 and 17*), appear to show a concentration of violations of Articles 5, 6 (consent), 13 (transparency) and 32 (security) GDPR.

Privacy Sanction Radar



GDPR: Highest Economic Sanctions

RANK	COUNTRY	ORGANIZATION	DATE	SANCTION (EURO)	ARTICLES VIOLATED (GDPR)
1	France	Google Inc.	January 2019	50.000.000	5, 6, 13, 14
2	Germany	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	October 2020	35.258.707,95	5, 6
3	Italy	TIM S.p.A.	February 2020	27.800.000	5, 6, 7, 12, 13, 21, 23, 24, 28, 32, 33
4	United Kingdom	British Airways	October 2020	22.073.000*	5, 32
5	United Kingdom	Marriott International	October 2020	20.421.600*	32
6	Italy	Wind Tre S.p.A.	July 2020	16.700.000	5, 6, 12, 24, 25
7	Italy	Vodafone Italia S.p.A.	November 2020	12.251.601	5, 6, 7, 15, 16, 21, 24, 25, 32, 33
8	Italy	ENI Gas e Luce	January 2020	11.500.000	5, 6, 7, 25, 32
9	Germany	Notebooksbilliger.de	December 2020	10.400.000	5, 6
10	Spain	Vodafone España, S.A.U	March 2021	8.150.000	21, 24, 28, 44

Better late than never?



In April 2021, the Dutch DPA fined *Booking.com* EUR 475.000 reporting a data breach with a delay of **22 days**.

In March 2021, the Spanish DPA fined *Air Europa Lineas Aereas* EUR 600.000. The data breach had been notified with a delay of **41 days**.

Data security: Additional recent fines

- **EUR 423.000** fine to *Virgin Mobile Polska* for failure to implement appropriate technical and organizational measures (Poland, December 2020).
- **EUR 440.000** fine to Amsterdam-based hospital *OLVG* due to inadequate protection of patient medical records (the Netherlands, February 2021).
- **GBP 1,25 million** fine to *Ticketmaster UK Limited* for breach of payment details (UK, November 2020).





Methodology to create an integrated privacy and cybersecurity compliance framework

Privacy and Cybersecurity European Legal Actual Framework

General Data Protection Regulation

- Companies that process personal data

The NIS Directive

- Operators of Essential Services and Digital Service Providers

Cybersecurity Act

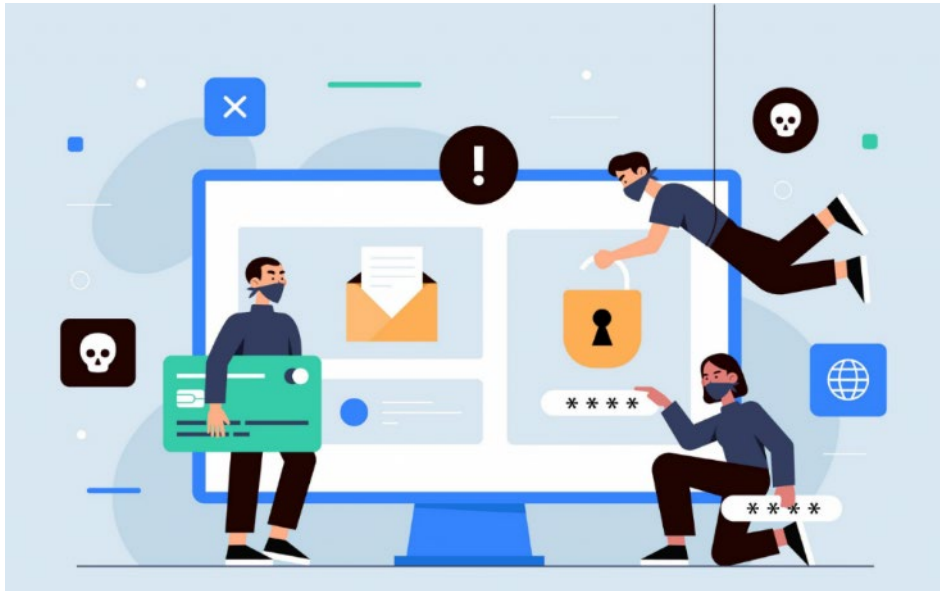
- Products

European Electronic Communications Code

- Communication providers and digital service providers

Privacy and Cybersecurity European Legal Future Framework

The NIS Directive 2



One of the most important innovations is undoubtedly the attention that the proposed NIS 2 Directive pays to the need to ensure the security of the so-called supply chain, which is expressly mentioned in the minimum measures to be imposed on important and essential entities.

Privacy and Cybersecurity European Legal Future Framework



The NIS Directive 2

NIS 2 is focused on the profound interconnection and integration that characterizes the current IT scenario, recognizing that strategically important entities often depend on third-party suppliers for aspects linked to networks and information systems.

Privacy and Cybersecurity European Legal Future Framework



The NIS Directive 2 and GDPR: Third parties

The proposed NIS 2 Directive, in dedicating space to the need to assess and take into account, from a security point of view, the quality and development of products and services, as well as the procedures of third-party suppliers and any related vulnerabilities, is in line with what has already been established, in the field of personal data protection, by the GDPR.

Privacy and Cybersecurity European Legal Future Framework

The NIS Directive 2 and GDPR: Third parties

In fact, the GDPR, where data processing is entrusted to third parties as data processors, not only requires the conclusion of appropriate contractual measures but also requires data controllers to conduct a prior assessment of suppliers and the security measures they have adopted.

This practice is further strengthened by this proposed Directive.



Methodology to create an integrated privacy and cybersecurity compliance framework

Taking into consideration that although the EU legislator can strengthen the principles and create obligations to protect the company's information assets and consequently the critical infrastructures and essential services of the Member States, from an operational point of view there is no change that can be obtained only through regulations.

In fact, the regulatory framework has the function of reinforcing awareness related to cybersecurity and imposing sanctions where necessary but leaving to other branches of human knowledge the solutions for the operational implementation of regulatory principles.

Methodology to create an integrated privacy and cybersecurity compliance framework

- Cybersecurity is **one** and is composed of many branches of human knowledge.
- It **exceeds** IT to encompass not only law but also the fields of
 - psychology,
 - engineering management,
 - communication.
- In this sense, the predisposition of an integrated compliance framework embraces **all the processes** of a company in a multidisciplinary approach based on **risk analysis**.



Methodology to create an integrated privacy and cybersecurity compliance framework

An integrated data protection and cybersecurity **governance system** can reduce the inefficiencies typical of an unstructured approach through a correct and timely identification and addressing of the real compliance and security needs of a company.

An **approach by processes** facilitates the task of identifying risks.

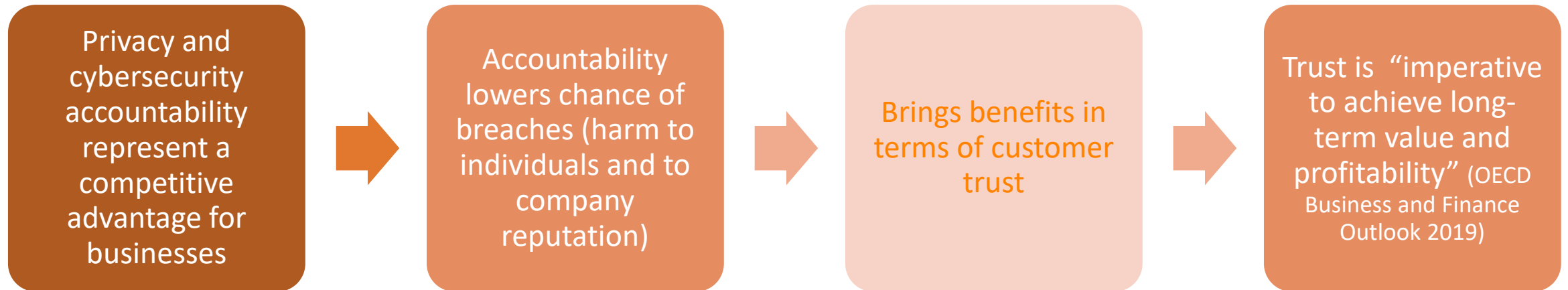
The first area of data protection and cybersecurity on which the company must invest is precisely that relating to **governance**.

It allows, on the one hand, to ensure an adequate and constant level of security, avoiding false perceptions of security and compliance, and on the other hand, to **optimize investments** concentrating them where effectively necessary.



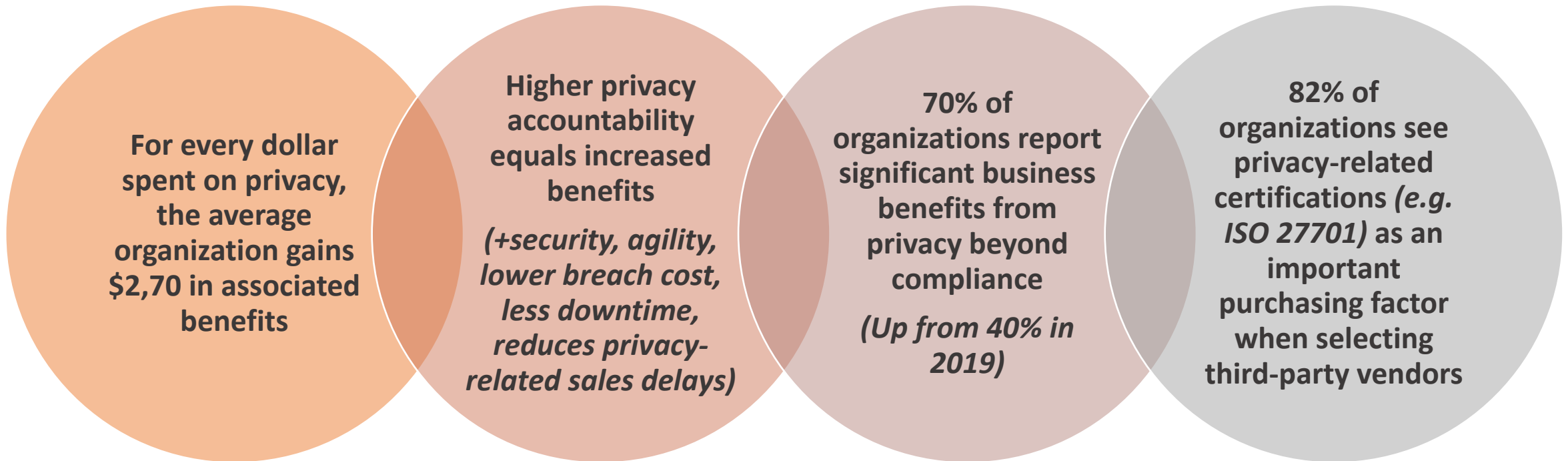
Quantifying Privacy ROI & Cybersecurity ROI

Privacy and cybersecurity are good for both business and people



Cisco Data Privacy Benchmark Study 2020 - *From Privacy to Profit: Achieving Positive Returns on Privacy Investments*
<https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?CCID=cc000160&DTID=esootr000515&OID=rptsc020143>

ROI of Privacy



See CISCO, From Privacy to Trust and ROI
<https://blogs.cisco.com/security/from-privacy-to-profit>

ROSI - Return On Security Investment

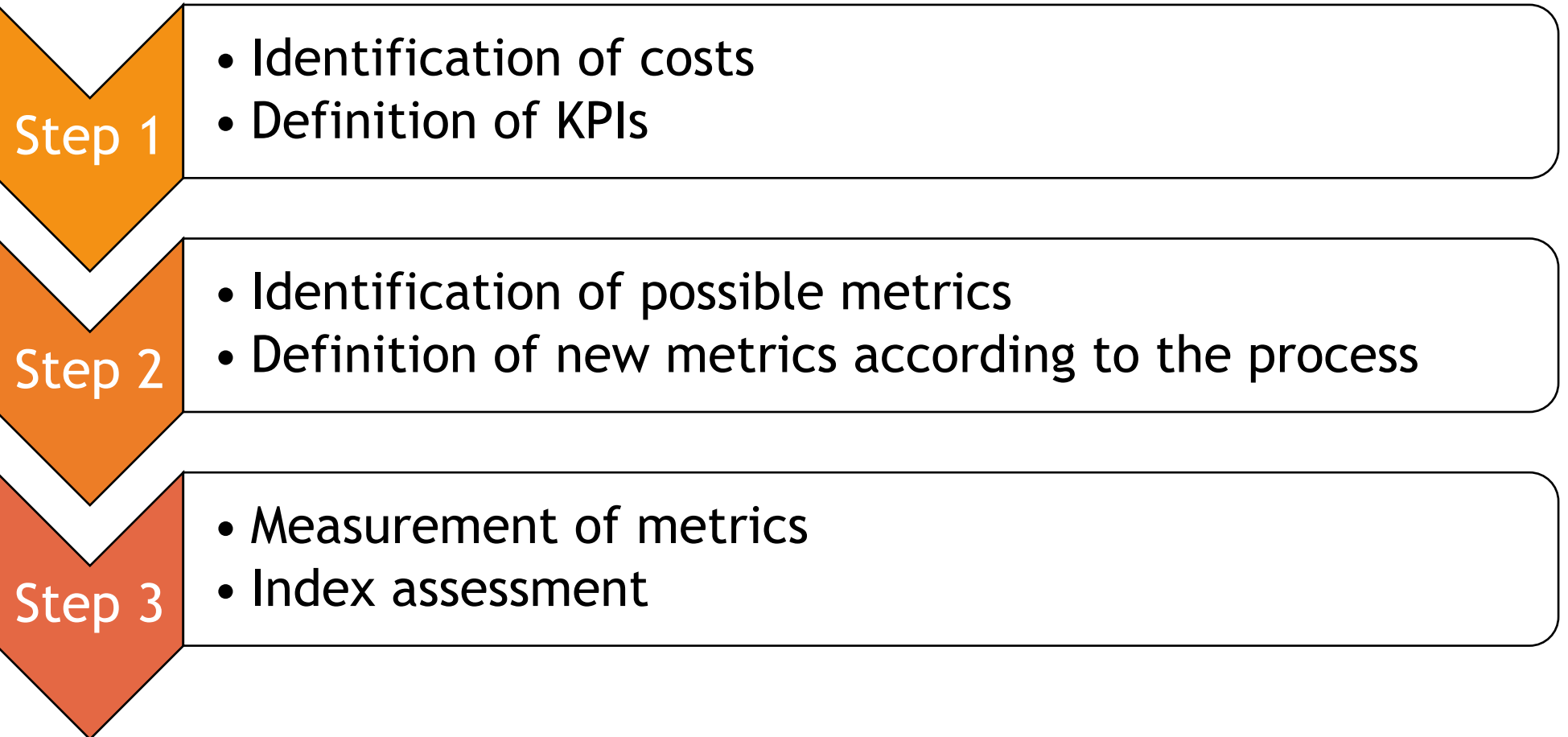
In recent years, numerous attempts have been made to define a scientific/mathematical method to calculate the costs and **returns of investments** in security initiatives.

The assessment of costs and returns or the calculation of ROSI involves the **identification and measurement of two main types of indicators**.

Key Cost Indicator: index used to measure the performance of processes, useful for calculating the cost.

Key Return Indicator: index used to measure the performance of processes, useful to calculate the return and justify the investment in security.

ROSI - Return On Security Investment



The background of the slide is a dark, textured composition. On the left, a hand is shown holding a smartphone. The entire scene is overlaid with a complex network of glowing orange lines and dots, resembling a digital or data network. The text 'Conclusions & recommendations' is centered in a large, white, sans-serif font.

Conclusions & recommendations

Cyber-Data Security Take-aways

- Data Security is the **#1 single cause of sanctions under the GDPR**.
- Adequate security is not only a question of financial risk, but also of *reputation* and *trust*.
- **In order to succeed in the increasingly competitive (and attack-prone) global market, reassuring clients and business partners of your cyber-data-security positioning will be key.**
- Research shows that investing in Data security furthers ROI.
- **Data security is no longer only a *compliance requirement* - it is a *business requirement* and will increasingly be seen as part of **CSR** - see the Maastricht University Data Protection as a Corporate Social Responsibility Project (UM DPCSR) with Principle 1, Rule 1: *Implement Data Security by Design*. The Organization shall implement Data Security by Design into its data processing activities.**



Thank you for your attention!



Prof. Dr. Paolo Balboni - Founding Partner ICTLC

Professor of Privacy, Cybersecurity, and IT Contract Law at
the European Centre for Privacy & Cybersecurity at Maastricht University
E: paolo.balboni@ictlegalconsulting.com / Twitter: @balbonipaolo

Helaine Leggat - Managing Partner - ICTLC Australia

Attorney at Law, CISSP, CISM, CIPP, CIPT, GAICD
E: helaine.leggat@ictlegalconsulting.com / Twitter: @helaineleggat

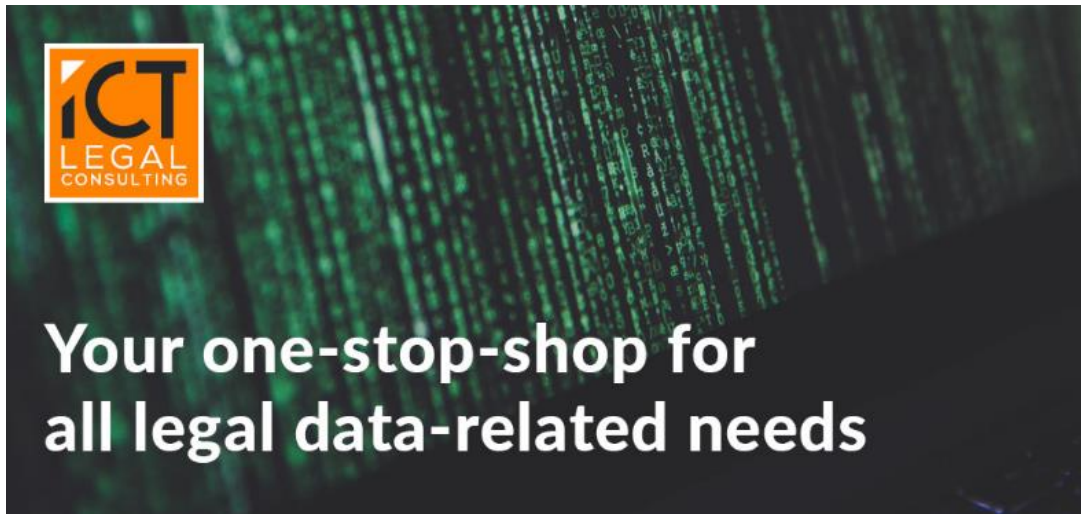
Francesco Capparelli - Chief Cyber Security Advisor ICTLC

Chief Cyber Security Advisor ICT Cyber Consulting - Senior
E: francesco.capparelli@ictcyberconsulting.com / Twitter: @FraKrelli

Milan - Bologna - Rome - Amsterdam - Melbourne - Madrid - Helsinki

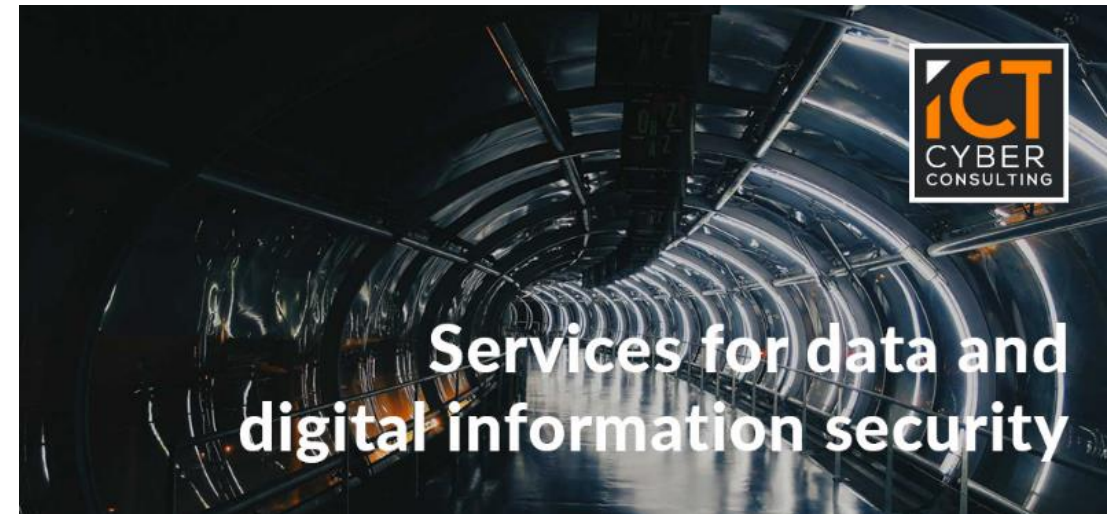


ICTLC is an international consulting firm that offers ***all-inclusive advice*** to organisations that deal with the challenges and opportunities of the digital era on a daily basis.



ICT Legal Consulting is a law firm specialised in the fields of Information and Communication Technology, Privacy, Data Protection and Intellectual Property Law.

The team draws on the experience of two firms, ICT Legal Consulting and ICT Cyber Consulting, which over the years have acquired consolidated experience and obtained demonstrable results in their respective fields.



ICT Cyber Consulting is a company specialized in the ***provision of cybersecurity services*** and technological data protection by design.

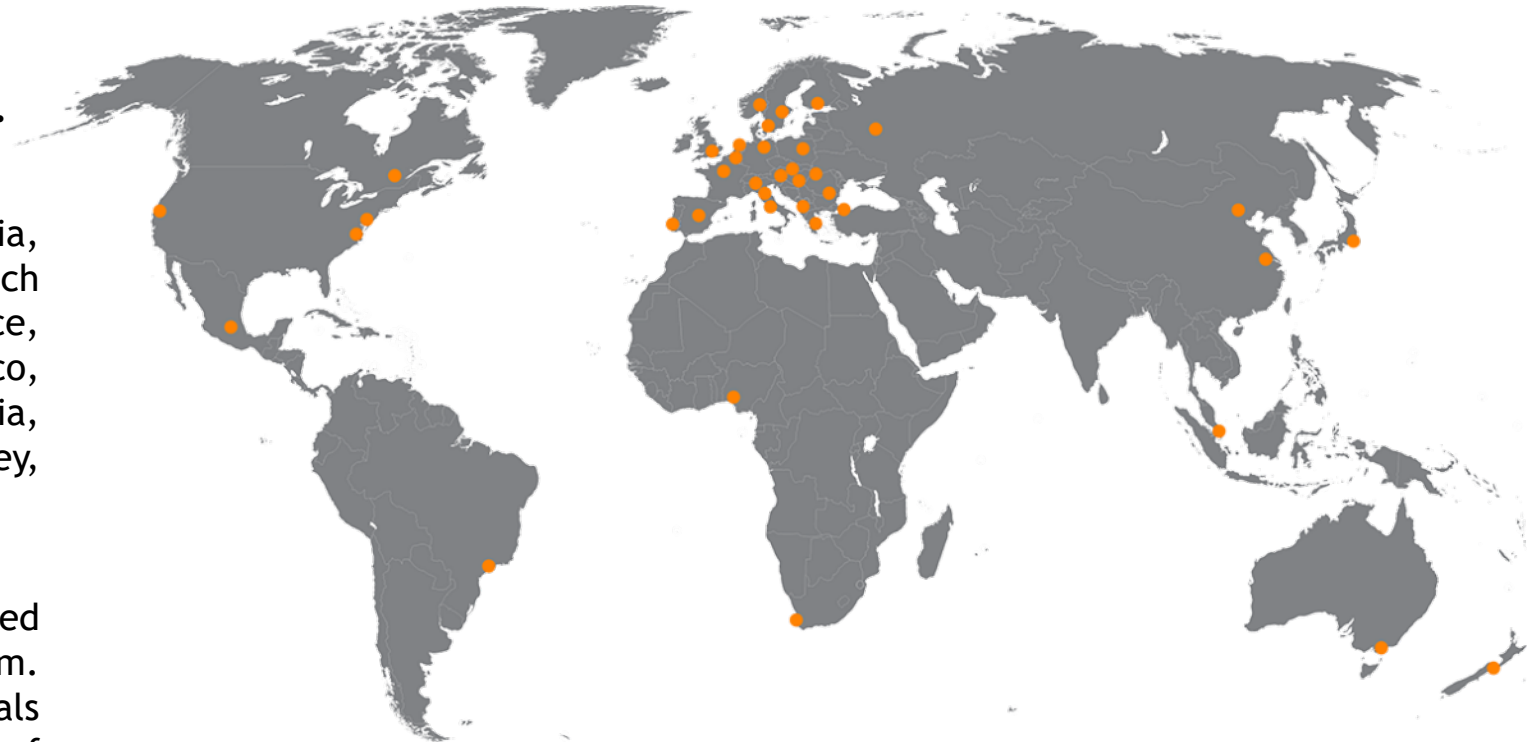


ICT Legal Consulting

ICT Legal Consulting is an international law firm with offices in **Milan, Bologna, Rome, Madrid, Amsterdam, Helsinki and Melbourne.**

The firm is present in **33 other countries**: Albania, Austria, Belgium, Brazil, Bulgaria, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Luxembourg, Macedonia, Mexico, Moldova, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Sweden, Switzerland, Turkey, the United Kingdom and the United States.

In each of these countries we have established partnerships with more than one law firm. Depending on the task, we contact the professionals who are best able to meet the specific needs of customers.





In Detail

ICT Legal Consulting is an **international law firm**. It was established by **Paolo Balboni** and **Luca Bolognini**, who have successfully assembled a network of trusted, highly-skilled lawyers and cyber security advisors specialized in the fields of Information and Communication Technology, Privacy, Data Protection/Security and Intellectual Property.

We have developed significant expertise working with multinationals and other companies in the communications, media & entertainment, IT, healthcare, pharmaceutical, fashion, food & beverage, energetic and smart grids, banking/financial services, automotive, industrial manufacturing and e-government sectors, as well as with public bodies and NGOs.

In more detail, we provide complete assistance in the fields of personal data protection (also acting as external DPO), IT contracts, eHealth, eCommerce, Direct Marketing, online advertising, cloud and edge computing, web 2.0 service provider liability, internet and mobile content, Artificial Intelligence, Internet of Things, electronic signatures, digital document retention and online storage, administrative responsibility and corporate liability. We focus on Next Generation IoT, Connected Vehicles, RPA Robotic Process Automation, robotics, distributed ledgers & blockchain, Artificial Intelligence, Data Valorisation, Data Monetization, Fintech, PSD2, Paytech, Big Data Protection, Data Protection by Design, Legal Design, Secondary Use of Data for Scientific Research, Synthetic Data, Multijurisdictional GDPR Compliance projects, Intercompany Data-Sharing Agreements, Transfer Impact Assessments (TIAs), Joint Controlling Agreements, ePrivacy regulation, Data-Driven Market general and sectorial regulation, Digital Services regulation, Ethics and Data Protection Impact Assessments (EDPIAs), Legitimate Interest Assessment (LIAs), IT and System Integration Contracts, IT/OT Outsourcing Services contracts, Service and Privacy Level Agreements (SLAs, PLAs), Legal-Cybersecurity Integrated Advice, Data Governance Models.

We also deal with the protection and management of intellectual property and competition rights: copyright, design, patents, unfair competition, consumer protection and media law, unfair commercial practices, misleading and comparative advertising, the labeling and sale of foodstuffs.

Our professionals regularly advise multinational companies on **legal and technical issues**, offering a **strategic and holistic approach**. Our goal is to **turn legal advice into a competitive advantage** for our clients.



Privacy and data protection



Cloud Computing



E-commerce



Information Technology



Cybersecurity



Big Data & Analytics



Internet of Things



Intellectual property



Marketing and advertising



Labor law



Telecommunications



E-Health

Our History

- 2011 ICTLC is founded by P. Balboni and L. Bolognini in Milan
- 2012 Inauguration of the Bologna office
- 2013 The Rome office is operational
- 2014 The international hub is established in Amsterdam
- 2015 Our services are offered in 21 countries
- 2016 The IT/Security practice is launched
- 2017 The new Milan office is operational
- 2018 Over 45 high-skilled professionals are active worldwide
- 2019 The Helsinki (Finland) office is operational
- 2020 ICTLC Australia and ICTLC Spain are established

The People



ICT Legal Consulting relies on more than 80 highly-skilled lawyers worldwide to carry out our clients' daily operations.

We are capable of scaling up anytime required. The core team consists of 50 selected professionals.



Paolo Balboni

Prof. Dr. Founding Partner



Paolo Balboni (Ph.D.) is a top tier European ICT, Privacy & Cybersecurity lawyer and serves as Data Protection Officer (DPO) for multinational companies. Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law. Member of the EUMETSAT Data Protection Supervisory Authority. Lead Auditor BS ISO/IEC 27001:2013.

Dr. Balboni (qualified lawyer admitted to the Milan Bar and the Amsterdam Bar) is a Founding Partner of ICT Legal Consulting (ICTLC), a law firm with offices in Milan, Bologna, Rome, Amsterdam, Helsinki, Madrid, Melbourne and Partner Law Firms in 33 countries around the world. Paolo Balboni is also Founding Partner of ICT Cyber Consulting, a company specialized in information/data security.

Together with his team he advises clients on legal issues related to cybersecurity, privacy and data protection, IT contracts, cloud/edge/quantum computing, artificial intelligence (AI), big data and smart analytics, internet of things (IoT), regulatory issues related to telecommunications and electronic communications, payments, e-commerce, digital marketing and advertising, regulations and liabilities of digital platforms, e-health, and general IP matters. He has long-term expertise in the ICT, Food and Beverage, Entertainment, Education, Healthcare, Automotive, Logistics and Transportation Solutions, Fashion, Human Resources Management, Insurance, and Financial and Banking sectors, including Fintech, and with specific reference to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) matters. He is a Recommended Lawyer ranked by The Legal 500 EMEA 2021 in the areas of Data Privacy and Data Protection and Industry Focus: TMT. In 2019 he was appointed as a Member of the EUMETSAT Data Protection Supervisory Authority.

Paolo Balboni is involved in European Commission studies on new technologies and participated in the revision of the EU Commission proposal for a General Data Protection Regulation. He played an active role in the drafting of the European Union Commission Data Protection Code of Conduct for Cloud Service Providers. He co-chairs the Privacy Level Agreement (PLA) Working Group of Cloud Security Alliance and has acted as the legal counsel for the European Network and Information Security Agency (ENISA) projects on 'Cloud Computing Risk Assessment', 'Security and Resilience in Governmental Clouds', and 'Procure Secure: A guide to monitoring of security service levels in cloud contracts'.

Keynote speaker at numerous international conferences on the legal aspects of Cybersecurity, ICT contracts, Privacy & Data Protection matters; Paolo Balboni is also the author of the book Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers (T.M.C Asser Press), and of numerous journal articles published in leading international law reviews.

Graduated in Law at the University of Bologna (Italy) in 2002, Paolo Balboni completed his Ph.D. in Comparative Technology Law at Tilburg University (The Netherlands) in 2008. He speaks Italian, English and Dutch fluently and has good knowledge of French, Spanish, and German.





Helaine Leggat

Managing Partner ICTLC Australia



Helaine Leggat (qualified lawyer admitted to the Supreme Court of Victoria Australia) is the founder of ICT legal, risk and advisory businesses in South Africa and Australia, and the Managing Partner of the Australia Office of ICT Legal Consulting (ICTLC).

An internationally recognised expert with considerable experience in cyberlaw, cyber security, data privacy and protection, and governance.

Together with her team she advises government and private sector entities in banking, insurance, mining, emerging technologies, defence, education, health, utilities, retail, logistics, privacy and data protection, governance, consumer markets, telecommunications, and critical infrastructure.

A former Director of the Australian Information Security Association, Member of the Expert Network for the Australian Government Department of Industry Innovation and Science, Member of the Law Institute of Victoria, Graduate of the Australian Institute of Company Directors (GAICD) and Member of the Steering Group for the Active Cyber Defence Alliance (ACDA).

In addition to her legal qualifications, she is one of a few people in the world to hold the following sought-after credentials: A Certified Information Systems Security Professional (CISSP), Certified Information Systems Security Manager (CISM), Certified Information Privacy Professional (CIPP), Certified Information Technologist (CIPT), and Fellow of Information Privacy (FIP), International Association of Privacy Professionals.

Over 20 years her work has involved legal, security, records and data privacy audits and advice, and the implementation of law and standards into client environments. Recently she has been largely focused on third party assurance and supply chain risk in the financial sector and operationalising the Consumer Data Right in Australia.

Helaine is a contributing author of numerous articles published in Australia and internationally on the application of national legal systems to cyberspace, ethics, privacy and data protection, and information/hybrid warfare.

Helaine regularly presents at international conferences including in Australia, China and United States and has been actively engaged in teaching and knowledge transfer for government, the private sector and academia for many years. Helaine co-founded ICT law firm, Information Legal, in 2013 in Melbourne. Information Legal is now ICTLC Australia, part of the ICTLC global network of firms.

Helaine graduated in Law at the University of South Africa in 1990 and completed the transfer of her degree to practice in Australia through the University of Sydney in 2016.



Francesco Capparelli

Chief Cyber Security Advisor ICTLC



Qualified Lead Auditor ISO/IEC 27001, ISO 22301, ISO 37001, ISO 20000-1, Risk Manager ISO 31000 and Internal Auditor ISO 19011. He has achieved PRINCE2 and CIPP/E Project Manager certifications. He has a degree in Law and two Masters in Law at LUISS in Rome, in Competition and Innovation Law, with specialization in Privacy & Big Data, and in Cybersecurity, with specialization in Artificial Intelligence and Biometrics. He also has a Master degree in Business Administration in Blockchain and Cryptocurrency Economics from Link Campus University with specialization in Smart Contract.


He is the Chief Cybersecurity Advisor of ICT Cyber Consulting, a legal-cybersecurity consulting firm, born as a spin-off of the ICT Legal Consulting, firm founded by Luca Bolognini and Paolo Balboni. ICT Cyber Consulting provides consultancy to multinationals and large companies on the topics of legal compliance on cybersecurity issues (GDPR, NIS, Cyber Perimeter, Telco, 231/01).

He coordinates the team of researchers and follows the activities related to research projects in the Horizon 2020 framework for the Italian Institute for Privacy, for which he has been a researcher since 2016 and is currently Senior Research Fellow. In addition, he is a lecturer in the Academy of the Institute, where he teaches in the course "Cybersecurity" and in the course "Master of Data Protection & Data Protection Designer®", sponsored by the Italian Data Protection Authority.


He also teaches at the Master in Cybersecurity of LUISS Guido Carli, within the framework of collaboration with ITHUM s.r.l., in the subjects related to the protection of personal data and legal cybersecurity, as well as in the courses of Alta Formazione Giuridica Economica (AFGE) in relation to the themes of computer security from the organizational point of view.

He is among the authors of the Code of Privacy Discipline (Giuffrè Francis Lefebvre, 2019), a work directed by Luca Bolognini and Enrico Pelino, within which he dealt with the transposition of the EU Directive 2016/1148 "NIS" within the Legislative Decree 65/2018 and the articles of the EU Regulation 2016/679 concerning the security of processing and the principle of accountability, in addition to the specific Measures of the Italian Data Protection Authority impacting on cybersecurity. He is among the authors of "Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection" (Now Publishers, 2020). He is also among the authors of the publication edited by Luca Bolognini, Privacy e libero mercato digitale (Giuffrè Francis Lefebvre, 2021) in which he dealt with the impact of IoT technologies on cryptocurrency and cybersecurity issues. He is the author of specialized articles and research papers related to the protection of personal data and cybersecurity such as "Terrorism: recognizing it to prevent it" for the Magna Carta foundation, which later became the subject of a bill on biometrics.





SERVICES | INDUSTRIES | ICT INSIDER | ABOUT US



The ECHR clarified the limits of corporate email snooping by employers

On September 5th, 2017, the Grand Chamber of the European Court of Human Rights declared that employees must be aware in advance of the monitoring of their corporate email account.

[Read more >](#)



SERVICES | INDUSTRIES | ICT INSIDER | ABOUT US




Privacy Regulation: new Study for possible changes to EC Proposal

Download the complete Study published by the Italian Institute for Privacy and Data Valorisation (Luca Bolognini, Camilla Bistolfi and Giovanni Crea).

[Read more >](#)



SERVICES | INDUSTRIES | ICT INSIDER | ABOUT US



WP29 on the Cooperation Procedure for the approval of the Binding Corporate Rules for controllers and processors

On April 11th 2018 the Article 29 Working Party, with the aim of providing a smooth and effective cooperation procedure in line with the EU General Data Protection Regulation, published a Working Document on the approval of Binding Corporate Rules for controllers and processors.

[Read more >](#)



SERVICES | INDUSTRIES | ICT INSIDER | ABOUT US



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

The Italian Data Protection Authority's FAQs on the Data Protection Officer (DPO) in the private sphere

FAQs are a useful tool that can serve as a more specific guidance, in addition to the Article 29 Working Party ("WP29") Opinion on DPOs, to further clarify the DPO role in the private sector.

[Read more >](#)



Awards

ICT Legal Consulting has been ranked by **The Legal 500 EMEA 2021** in the Top Tier of the **Data Privacy and Data Protection** (Italy) practice area. Both of our Founding Partners **Paolo Balboni** and **Luca Bolognini** are Recommended Lawyers, alongside the Partners **Nicola Franchetto** and **Vito Michele Pavese**. Luca Bolognini has also been listed as a “Leading Individual” and **Vito Michele Pavese** as “Next Generation Partner”.

In the **Industry focus: TMT** practice area (Italy), both our Founding Partners **Luca Bolognini** and **Paolo Balboni** have been listed as Recommended Lawyers.

Read more at legal500.com/ict-legal-consulting/milan-Italy.



Awards





ICT Cyber Consulting

*Data and information security
consulting services*



ICT Cyber Consulting

*Data and information security
consulting services*



ICT Cyber Consulting was born as a spin-off of ICTLC - ICT Legal Consulting firm, with the aim of providing guidance, assistance and quality services to companies and to entities in terms of cybersecurity, technology and data protection. The security of data and information, particularly where new technologies are involved, is an integral part of requirements of the utmost importance, that derive from numerous and diverse norms. Not only because of the GDPR (EU General Data Protection Regulation) and the NIS (Network and Information Security) Regulations, but also in regard to the field of trade and industrial secret, which always require setting major attention and effort in particular towards the levels of adequacy of ICT security.

Some of our services:

1. **NIS Gap Analysis & Compliance Action Plan**
2. **Cybersecurity Gap Analysis**
3. **Cybersecurity alignment to GDPR**
4. **Hotline Cybersecurity & Data Breach Management Unit**
5. **Data Protection Impact Assessment - Cybersecurity**
6. **Cybersecurity assessment of applications**
7. **Verification of ISO/IEC 27001:2013 controls (Information Security)**
8. **Verification of ISO 22301:2019 controls (Business Continuity)**
9. **Verification of ISO 37001:2019 controls (Anti-Bribery)**
10. **Management and configuration Privacy by Design**
11. **Offensive Services (VA, PT, Phishing, Osint, Red Teaming)**
12. **Security Assessment external suppliers**
13. **GDPR second part audits**
14. **Training**



Contacts

Milan

Via Borgonuovo, 12
20121 - Milan - Italy
Phone: +39 02 84247194
Fax: +39 02 700512101

Bologna

Via Ugo Bassi, 3
40121 - Bologna - Italy
Phone: +39 051 272036
Fax: +39 051 272036

Rome

P.zza di San Salvatore in Lauro, 13
00186 - Rome - Italy
Phone: +39 06 97842491
Fax: +39 06 23328983

International

Piet Heinkade 55
1019 GM Amsterdam
The Netherlands
Phone: +31 (0)20 894 6338

Madrid

Calle de Alcalá, 75
28009 - Madrid
Spain
Phone: +34 91 577 50 20

Helsinki

Neitsytpolku 5 B 49
00140 - Helsinki
Finland
Phone: +358 50 4801292

Melbourne

Clarence Chambers, Level 11
456 Lonsdale Street, Melbourne VIC 3000
Australia
Phone: +61 (03) 9070 9847

ICTLC is present in further 33 countries: Albania, Austria, Belgium, Brazil, Bulgaria, Canada, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Japan, Luxembourg, North Macedonia, Mexico, Moldova, New Zealand, Nigeria, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, Sweden, Switzerland, Turkey, United Kingdom and the United States.

Follow us on:



Email contact

info@ictlegalconsulting.com