





*CSI Piemonte*  
Certificazioni GDPR e Codici di condotta:  
a che punto siamo  
29 settembre 2022

## CSA's Code of Conduct for GDPR compliance

---

Paolo Balboni - Founding Partner  
paolo.balboni@ictlegalconsulting.com

Milano - Bologna - Roma - Amsterdam - Atene - Helsinki - Madrid - Melbourne



# Interesting developments in the cloud domain: CoCs (Art. 40 GDPR)

[20 May 2021 - During its plenary session, the EDPB adopted two Art. 64 GDPR opinions \(see Op.1 and Op.2\) on the first draft decisions on transnational Codes of Conduct \(Codes\) presented to the Board by the Belgian and French supervisory authorities \(SAs\).](#)

In particular, the Belgian SA's draft decision concerns the [EU CLOUD Code of conduct](#), addressed to **cloud service providers**. (see [EDPB opinion](#))

The French SA's draft decision concerns the [CISPE Code of conduct](#), addressed to cloud **infrastructure** service providers. (see [EDPB opinion](#))

These Codes aim to provide practical guidance and define specific requirements (i.e. Art. 28 GDPR) for **processors** in the EU subject to these Codes. They are not to be used in the context of international transfers of personal data. The EDPB is of the opinion that both draft codes comply with the GDPR and fulfil the requirements set forth in Art. 40 and 41 GDPR. According to the GDPR, adherence to approved codes of conduct may be used as an element to demonstrate legal compliance.

EDPB Chair, Andrea Jelinek said: *“We welcome the efforts made by the code owners to elaborate codes of conduct, which are practical, transparent and potentially cost-effective tools to ensure greater consistency among a sector and foster data protection compliance.”*

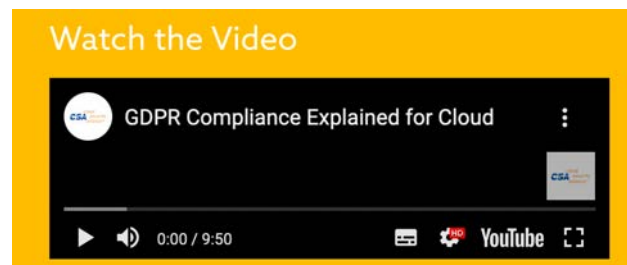


# Interesting developments in the cloud domain: CoCs (Art. 40 GDPR)

CSA has also developed a Code of Conduct “[CSA CoC for GDPR Compliance](#)” which is also under the evaluation of the EDPB (French DPA-CNIL as lead authority)

The CoC helps:

- a. cloud service providers (CSPs) determine the level of protection they are required to provide; and
- b. offers cloud customers a tool to evaluate the level of personal data protection offered by a CSP



## Interesting developments in the cloud domain: EUCS – Cloud Services Scheme

This publication is a draft version of the EUCS candidate scheme (**European Cybersecurity Certification Scheme for Cloud Services**), which looks into the certification of the cybersecurity of cloud services. In accordance with Article 48.2 of the Cybersecurity Act1 (EUCSA), ENISA has set up an Ad Hoc Working Group (AHWG) to work on the preparation of the candidate scheme on cloud services, as part of the European Cybersecurity Certification Framework. This is a draft version to be used as basis for an external review. The objective of the review is to validate the principles and general organization of the proposed scheme, and to gather feedback on the proposed wording of the sections and annexes.



90,000+

INDIVIDUAL  
MEMBERS

75+

CHAPTERS

300+

CORPORATE  
MEMBERS

30+

ACTIVE WORKING  
GROUPS

Strategic partnerships with governments, research institutions, professional associations and industry

Active role in the standardization community: Liaison with ISO SC 27 and SC38

CSA research is FREE!

2009

CSA FOUNDED



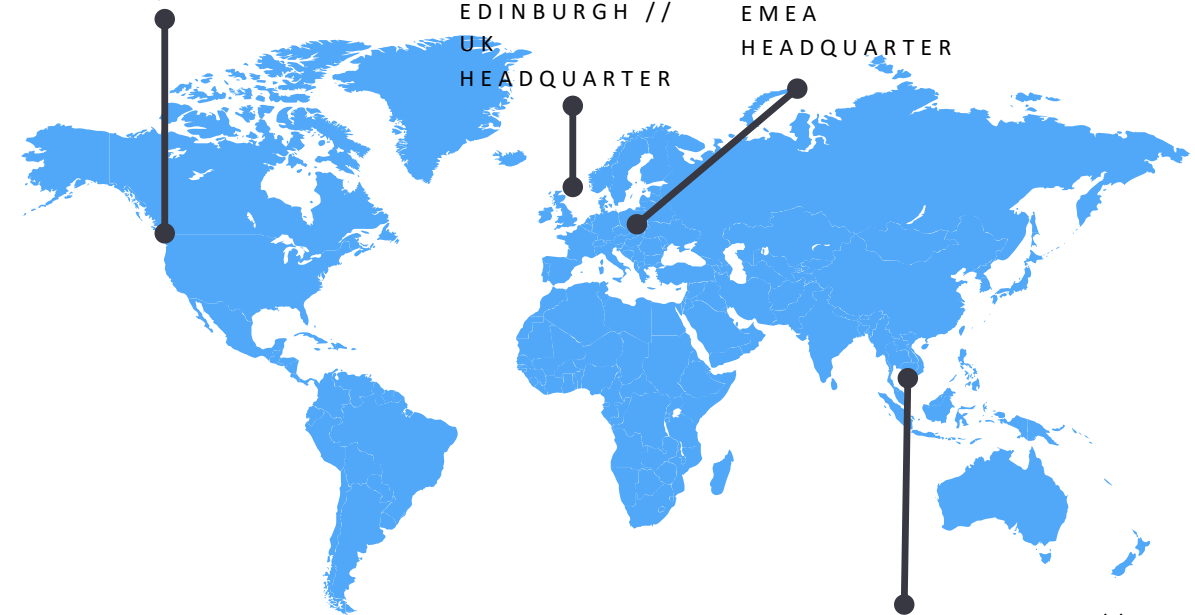
OUR Community

SEATTLE/Bellingham, WA //  
US HEADQUARTERS

EDINBURGH //  
UK  
HEADQUARTER

EDINBURGH //  
EMEA  
HEADQUARTER

SINGAPORE //  
ASIA PACIFIC  
HEADQUARTER



# CODES OF CONDUCTS & CERTIFICATION

---



The Regulation “encourages” the use of:

- **codes of conducts** and
- **certification mechanisms**



**SCOPE:** to ensure **transparency** and **compliance** to the law

## CSA CODE OF CONDUCT: GOALS



- Provide **CSPs** a tool to **achieve GDPR compliance** and **demonstrate** it through **SELF-ATTESTATION** or **THIRD-PARTY ASSESSMENT**
- Provide **CLOUD CUSTOMERS** with a tool to **EVALUATE** the level of **CSP Data Protection COMPLIANCE**





# CSA CODE OF CONDUCT: SCOPE & STRUCTURE

- Structured in **3 components**:

**1**  
CSA CoC Objectives,  
Scope, Methodology,  
Assumptions &  
Explanatory Notes

**2**  
CSA CoC Control  
Specifications:  
Privacy Level  
Agreement

**3**  
CSA Code of Conduct  
Governance and  
Adherence  
Mechanisms

- Deals with the 'B2B' scenario (**'B2C' is out-of-scope**)
- Detailed list of GDPR requirements + additional best practices for the cloud sector
- Strongly based on opinions/guidelines of the European Data Protection Board (former WP29), European Data Protection Supervisor, national supervisory authorities and ENISA, as well as ISO standards
- Considers role of CSPs as "controllers", "processors", "joint-controllers" and "sub-processors"



PRIVACY LEVEL AGREEMENT WORKING GROUP, NOVEMBER 2017





# CSA CODE OF CONDUCT: SCOPE & STRUCTURE

CSA<sup>®</sup>

1

## CSA CoC Objectives, Scope, Methodology, Assumptions & Explanatory Notes

CSA CoC can be adhered to by **CSPs**, regarding **one or more of the services they provide.**

The CoC refers to services provided by a CSP, not the CSP itself!





# CSA CODE OF CONDUCT: SCOPE & STRUCTURE <sup>CSA</sup>

## 1 CSA CoC Objectives, Scope, Methodology, Assumptions & Explanatory Notes

CSA CoC can be referenced or used as an **appendix to a service agreement.**

Describe the level of privacy protection which the CSP will provide, in connection with certain services



# CSA CODE OF CONDUCT: SCOPE & STRUCTURE <sup>CSA</sup>

## 1 CSA CoC Objectives, Scope, Methodology, Assumptions & Explanatory Notes

CSA CoC aims to create additional value for **CSPs, cloud customers, data subjects** and the **cloud community at large**

- Organic, structured and systematic Identification of all relevant GDPR provisions for CSPs;
- Explanation of those provisions and their relevance, when applied to cloud computing;
- Raising the bar for data protection and privacy in cloud computing, by adding additional controls.

# Controller – Processor (CSP)

In response to feedback received from the CNIL (the French Supervisory Authority, which is leading on the CSA CoC approval process), CSA has decided to restrict the CoC's scope, for approval purposes, to **CSPs acting as PROCESSORS**.



However, the ultimate goal – to develop a CoC with enforceable obligations upon all CSPs, acting as **CONTROLLERS** or **PROCESSORS** – remains unchanged.

# REQUIREMENTS

1	CSP declaration of compliance and accountability	9	Data portability, migration, and transfer back
2	CSP relevant contacts and its role	10	Restriction of processing
3	Ways in which the data will be processed	11	Data retention, restitution, and deletion policies
4	Record keeping	12	Cooperation with the cloud customers
5	Data transfer	13	Legally required disclosure
6	Data security measures	14	Remedies for cloud customers
7	Monitoring	15	CSP insurance policy
8	Personal data breach		



# CONTROL SPECIFICATIONS

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
WAYS IN WHICH THE DATA WILL BE PROCESSED.			WWP-1.13	13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., report production) and those conducted at the CSP's initiative (e.g., backup, disaster recovery, fraud monitoring).	Applicable	Not Applicable
			WWP-1.14	CSPs that are <b>processors</b> provide to cloud customers details on:  14. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor (General Information - applicable to CSPs that are processors).		Applicable
			WWP-1.15	15. Specify how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors)	Applicable	Applicable
		2 Personal data location	WWP-2.1	1. Specify the location(s) of all data centres or other data processing locations (by country) where personal data may be processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means).	Applicable	Applicable
		3 Subcontractors	WWP-3.1	1. Identify subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.	Applicable	Applicable
			WWP-3.2	2. Declare to cloud customers that the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.	Not Applicable	Applicable
			WWP-3.3	3. Declare to cloud customers that the CSP imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law;	Not Applicable	Applicable

# CONCLUSIONS







# Paolo Balboni Prof. Dr - Founding Partner



Paolo Balboni (Ph.D.) è un avvocato esperto di diritto europeo delle nuove tecnologie, di privacy e cyber security. Fornisce servizi di Data Protection Officer (DPO) per società multinazionali. Paolo Balboni è Professore di Privacy, Cybersecurity, and IT Contract Law presso lo [European Centre on Privacy and Cybersecurity \(ECPC\)](#) della Facoltà di Giurisprudenza dell'Università di Maastricht. Membro dell'Autorità di controllo per la protezione dei dati personali di EUMETSAT. Lead Auditor BS ISO/IEC 27001:2013.

Avvocato del Foro di Milano e di Amsterdam, Paolo Balboni è Socio Fondatore di [ICT Legal Consulting \(ICTLC\)](#), studio legale internazionale con sedi a Milano, Bologna, Roma, Amsterdam, Atene, Helsinki, Madrid, Lagos, Melbourne e una rete di diversi studi legali partner in altri 48 paesi nel mondo. Paolo Balboni è anche Socio Fondatore di [ICT Cyber Consulting](#), società specializzata nella consulenza in materia di information/data security.

Insieme al suo team svolge attività di consulenza legale in materia di sicurezza informatica, privacy e protezione dei dati, contrattualistica IT, cloud/edge/quantum computing, artificial intelligence (AI), big data e smart analytics, internet of things (IoT), questioni normative relative alle telecomunicazioni e alle comunicazioni elettroniche, ai pagamenti, al commercio elettronico, al marketing digitale e alla pubblicità, alle normative e alle responsabilità delle piattaforme digitali, all'e-health e al diritto della proprietà intellettuale. Paolo Balboni vanta una notevole esperienza nei settori: ICT, industria alimentare, Intrattenimento, Istruzione, Sanità, Automotive, Logistica e Trasporti, Moda, Gestione delle risorse umane, Assicurazione, Istituzioni finanziarie, incluso Fintech, con specifico riferimento alle questioni di Anti-Money Laundering (AML) e Counter-Terrorist Financing (CFT). Professionista consigliato da "The Legal 500 EMEA 2021" per i settori "Data Privacy & Data Protection" e "Industry Focus: TMT". Dal 2019, è membro dell'Autorità di controllo per la protezione dei dati personali di [EUMETSAT](#).

Paolo Balboni è coinvolto in vari studi della Commissione Europea relativi alle nuove tecnologie e ha partecipato alla revisione della proposta della Commissione Europea di Regolamento generale sulla protezione dei dati. Paolo Balboni ha svolto un ruolo attivo nella redazione del Codice di Condotta della Commissione Europea per la protezione dei dati personali dei fornitori di servizi Cloud. È co-presidente del Gruppo di Lavoro su [Privacy Level Agreement \(PLA\)](#) di Cloud Security Alliance ed è stato Consulente legale scelto per i progetti dell'European Network and Information Security Agency (ENISA) su ['Cloud Computing Risk Assessment'](#), ['Security and Resilience in Governmental Clouds'](#), e ['Procure Secure: A guide to monitoring of security service levels in cloud contracts'](#).

Spesso invitato come "keynote speaker" a conferenze internazionali su aspetti legali di Cyber Security, contrattualistica ICT, Privacy & Data Protection; Paolo Balboni è anche autore del libro [Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers](#) (T.M.C Asser Press) e di numerosi articoli pubblicati sulle principali riviste di diritto internazionale.

Laureato in giurisprudenza all'Università di Bologna nel 2002, ha conseguito il dottorato (Ph.D.) in Diritto comparato delle nuove tecnologie all'Università di Tilburg (Paesi Bassi) nel 2008. Parla fluentemente in italiano, inglese e olandese ed ha una buona conoscenza delle lingue francese, spagnola e tedesca.

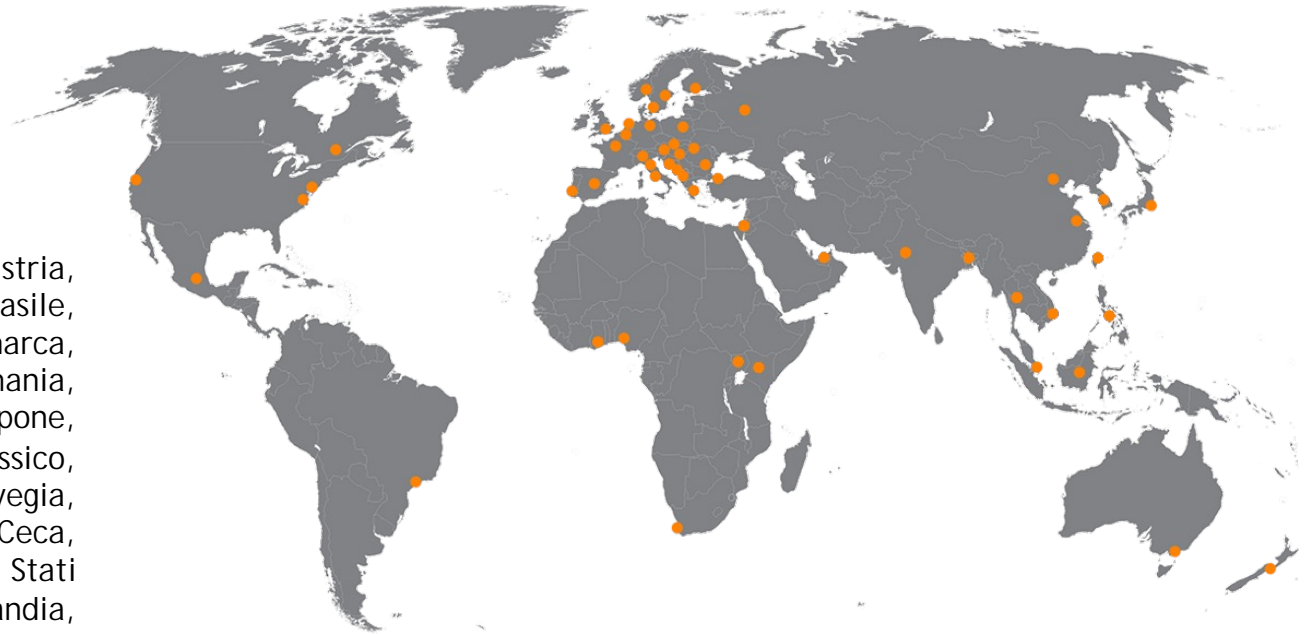




## Lo Studio

ICT Legal Consulting è uno studio legale internazionale fondato nel 2011 con sedi a **Milano, Bologna, Roma, Amsterdam, Atene, Helsinki, Madrid, Lagos e Melbourne.**

Siamo anche presenti **in altri 48 paesi**: Albania, Austria, Bangladesh, Belgio, Bosnia-Erzegovina, Brasile, Bulgaria, Canada, Cina, Corea del Sud, Danimarca, Emirati Arabi Uniti, Filippine, Francia, Germania, Ghana, India, Indonesia, Irlanda, Israele, Giappone, Kenya, Lussemburgo, Macedonia del Nord, Messico, Moldavia, Montenegro, Nuova Zelanda, Norvegia, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Romania, Russia, Serbia, Singapore, Slovacchia, Stati Uniti, Sudafrica, Svezia, Svizzera, Taiwan, Thailandia, Turchia, Uganda, Ungheria, Vietnam.



In ciascuno di questi paesi abbiamo stabilito partnership con più di uno studio legale. A seconda del compito, contattiamo i professionisti che sono maggiormente in grado di soddisfare le esigenze specifiche dei clienti.



# Nel Dettaglio

ICT Legal Consulting è uno **studio legale internazionale**. È stato fondato da **Paolo Balboni** e **Luca Bolognini**, i quali hanno raggruppato un team di fidati professionisti altamente qualificati e specializzati nei settori della tecnologia dell'informazione e della comunicazione, della privacy, della protezione dei dati, della sicurezza informatica e della proprietà intellettuale.

I nostri avvocati, insieme agli esperti di cybersecurity, svolgono attività di consulenza integrata 'Legale + Organizzativa + IT Security' per multinazionali e imprese innovative, enti pubblici e del Terzo Settore, principalmente in tema di protezione dei dati personali (anche in veste di DPO esternalizzati), contratti informatici, Intelligenza Artificiale, Internet delle Cose, RPA, e-health, e-commerce, marketing diretto, online advertising, cloud computing, responsabilità dei fornitori di servizi Web 2.0, responsabilità dei fornitori di contenuti su internet e terminali mobili, firme elettroniche e identità digitali, PSD2, gestione documentale e conservazione sostitutiva. Inoltre forniamo assistenza completa con riferimento alla tutela della proprietà intellettuale: diritto d'autore, marchi, design, brevetti, concorrenza sleale, protezione dei consumatori.

I nostri professionisti hanno sviluppato una considerevole esperienza nei seguenti settori economici e istituzionali: comunicazioni, media & entertainment, IT (specialmente: cloud computing, big data, analytics, Internet of Things), automotive, servizi sanitari, moda, energetico e smart grids, servizi bancari/finanziari ed e-government, responsabilità amministrativa penale d'impresa ex D.Lgs. 231/01, organizzazioni non governative, fondazioni pubbliche e casse di previdenza.

Lo studio fornisce regolarmente consulenze ad aziende multinazionali su **questioni legali e tecniche** offrendo un **approccio strategico e olistico** alla materia. Il nostro obiettivo è quello di trasformare la consulenza legale in un vantaggio competitivo per i nostri clienti.

# Principali Aree di Attività





## Servizi



Privacy e protezione  
dei dati personali



Cloud/Edge/Quantum  
computing



E- & M-commerce



Blockchain



Cybersecurity



Artificial Intelligence,  
Big Data & Smart Analytics



Internet of Things



Proprietà intellettuale/  
industriale



Marketing  
& Digital Advertising



Diritto del lavoro, compliance  
231, anticorruzione



Information & (Tele-)  
Communication Technology



E-Health



## La Storia

- 2011 ICT Legal Consulting è fondata da Paolo Balboni e Luca Bolognini a Milano
- 2012 Gli uffici di Bologna vengono inaugurati
- 2013 Apre la sede di Roma
- 2014 L'international desk apre ad Amsterdam
- 2015 I nostri servizi sono offerti in 21 paesi in tutto il mondo
- 2016 Viene lanciata la pratica IT / Security
- 2017 La nuova sede di Milano è operativa
- 2018 Nasce ICT Cyber Consulting, azienda spin-off specializzata in servizi di cybersecurity
- 2019 È aperta la sede ad Helsinki (Finlandia)
- 2020 ICTLC Australia e ICTLC Spagna sono inaugurate. ICT Legal Consulting diventa Europrivacy<sup>™/®</sup> Ambassador Partner\*
- 2021 Nasce ICTLC Grecia, con sede ad Atene

## Le Persone



ICT Legal Consulting si avvale di più di 80 avvocati altamente qualificati per assistere quotidianamente i propri clienti in tutto il mondo, ed è in grado di scalare la propria organizzazione a seconda delle esigenze.

Il team di base è costituito da 50 professionisti strutturati.

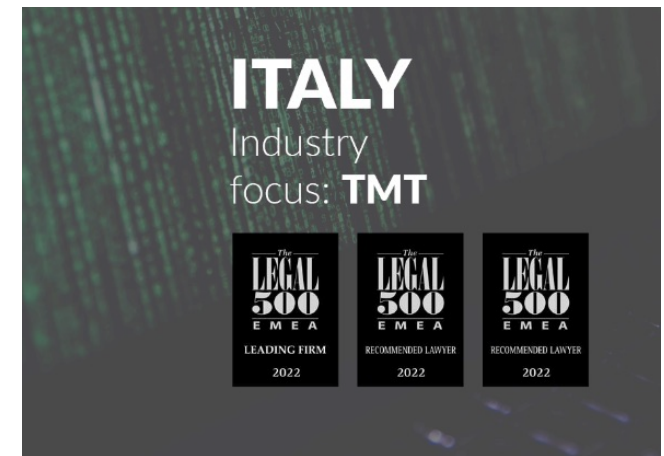


# Riconoscimenti

ICT Legal Consulting è stata segnalata da **The Legal 500 EMEA 2022** nel *Top Tier* della practice **Data Privacy and Data Protection** (Italia). Entrambi i nostri Founding Partners, **Paolo Balboni** e **Luca Bolognini**, sono stati riconosciuti come «Recommended Lawyer», come i nostri Partners **Floriana Francesconi** e **Vito Michele Pavese**. Luca Bolognini è stato inoltre selezionato come "Leading Individual" e **Vito Michele Pavese** è stato segnalato come "Next Generation Partner".

Nella practice **Industry focus: TMT** (Italia), entrambi i nostri Founding Partners, **Luca Bolognini** e **Paolo Balboni** sono stati segnalati come "Recommended Lawyer".

Per maggiori informazioni: [legal500.com/ict-legal-consulting/milan-Italy](https://legal500.com/ict-legal-consulting/milan-Italy).





# Riconoscimenti







# ICT *Cyber* Consulting

*Consulenza e servizi per la sicurezza  
dei dati e delle informazioni digitali*



# ICT Cyber Consulting

Consulenza e servizi per la sicurezza  
dei dati e delle informazioni digitali



ICT Cyber Consulting nasce come spin-off dello studio ICTLC - ICT Legal Consulting, con l'obiettivo di fornire orientamento, assistenza e servizi qualificati alle aziende e agli enti in materia di cybersecurity e *data protection by design* tecnologica. La sicurezza dei dati e delle informazioni, in particolare quando si utilizzano nuove tecnologie, è parte integrante di adempimenti di importanza critica, che derivano da numerose e differenti normative. Si pensi al GDPR (Regolamento Generale in materia di Protezione dei Dati UE), alla normativa NIS (Network and Information Security), ma anche ai campi di protezione del segreto aziendale e industriale, che richiedono sempre maggiori attenzioni e sforzi dedicati proprio ai livelli di adeguatezza della sicurezza ICT.

Alcuni dei nostri servizi di consulenza e assistenza cyber:

1. NIS Gap Analysis & Compliance Action Plan
2. Cybersecurity Gap Analysis
3. Allineamento cybersecurity GDPR
4. Hotline Cybersecurity & Data Breach Management Unit
5. Data Protection Impact Assessment - Cybersecurity
6. Valutazione cybersecurity degli applicativi
7. Controlli ISO/IEC 27001:2013 (Information Security)
8. Controlli ISO 22301:2019 (Business Continuity)
9. Controlli ISO 37001:2019 (Anti-Bribery)
10. Privacy by Design
11. Offensive Services (VA, PT, Phishing, Osint, Red Teaming)
12. Security Assessment fornitori esterni
13. Audit di seconda parte
14. Formazione



# Contatti

## Milano

Via Borgonuovo, 12  
20121 - Milano  
Italia  
Tel. +39 02 84247194

## Bologna

Via Ugo Bassi, 3  
40121 - Bologna  
Italia  
Tel. +39 051 272036

## Roma

P.zza di San Salvatore in Lauro, 13  
00186 - Roma  
Italia  
Tel. +39 06 97842491

## Amsterdam

Piet Heinkade 55  
1019 GM Amsterdam  
Paesi Bassi  
Tel. +31 (0)20 894 6338

## Atene

Ippokratous 8  
10679 Atene  
Grecia  
Tel. +30 210 3600366

## Madrid

Calle de Alcalá, 75  
28009 - Madrid  
Spagna  
Tel. +34 91 577 50 20

## Helsinki

Huopalahdentie 24  
00350 - Helsinki  
Finlandia  
Tel. +358 50 4801292

## Melbourne

Clarence Chambers, Level 11  
456 Lonsdale Street, Melbourne  
VIC 3000 - Australia  
Tel. +61 (03) 9070 9847

## Lagos

Aggey House - 12 Berkeley  
Street, Lagos Island - Lagos  
Nigeria  
Tel. +234 8150692572

ICT Legal Consulting é presente in altri 48 Paesi: Albania, Austria, Bangladesh, Belgio, Bosnia-Erzegovina, Brasile, Bulgaria, Canada, Cina, Corea del Sud, Danimarca, Emirati Arabi Uniti, Filippine, Francia, Germania, Ghana, India, Indonesia, Irlanda, Israele, Giappone, Kenya, Lussemburgo, Macedonia del Nord, Messico, Moldavia, Montenegro, Nuova Zelanda, Norvegia, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Romania, Russia, Serbia, Singapore, Slovacchia, Stati Uniti, Sudafrica, Svezia, Svizzera, Taiwan, Thailandia, Turchia, Uganda, Ungheria, Vietnam.

Follow us on:



Email contact  
[info.legal@ictlc.com](mailto:info.legal@ictlc.com)



# Grazie per l'attenzione!

**Paolo Balboni** - Founding Partner  
paolo.balboni@ictlegalconsulting.com

---

© 2022 ICT Legal Consulting - Tutti i diritti riservati. Ferme restando le utilizzazioni libere consentite dalle leggi vigenti, in mancanza di un'espressa autorizzazione scritta di ICT Legal Consulting è vietata qualunque riproduzione, utilizzazione o qualunque altra forma di messa a disposizione di terzi del presente documento o di una parte di esso.

---

info.legal@ictlc.com - www.ictlegalconsulting.com

"L'eccellenza non è un atto, ma un'abitudine" Aristotele