



ICTLC

YOUR ONE-STOP-SHOP FOR ALL  
DATA-RELATED NEEDS



# SOMMARIO

IL GRUPPO	<b>04</b>
LE SEDI	<b>06</b>
ICT LEGAL CONSULTING	<b>08</b>
I SERVIZI LEGALI	<b>16</b>
ICT CYBER CONSULTING	<b>30</b>
I SERVIZI CYBER	<b>32</b>
SETTORI	<b>46</b>



# IL GRUPPO

## ICTLC

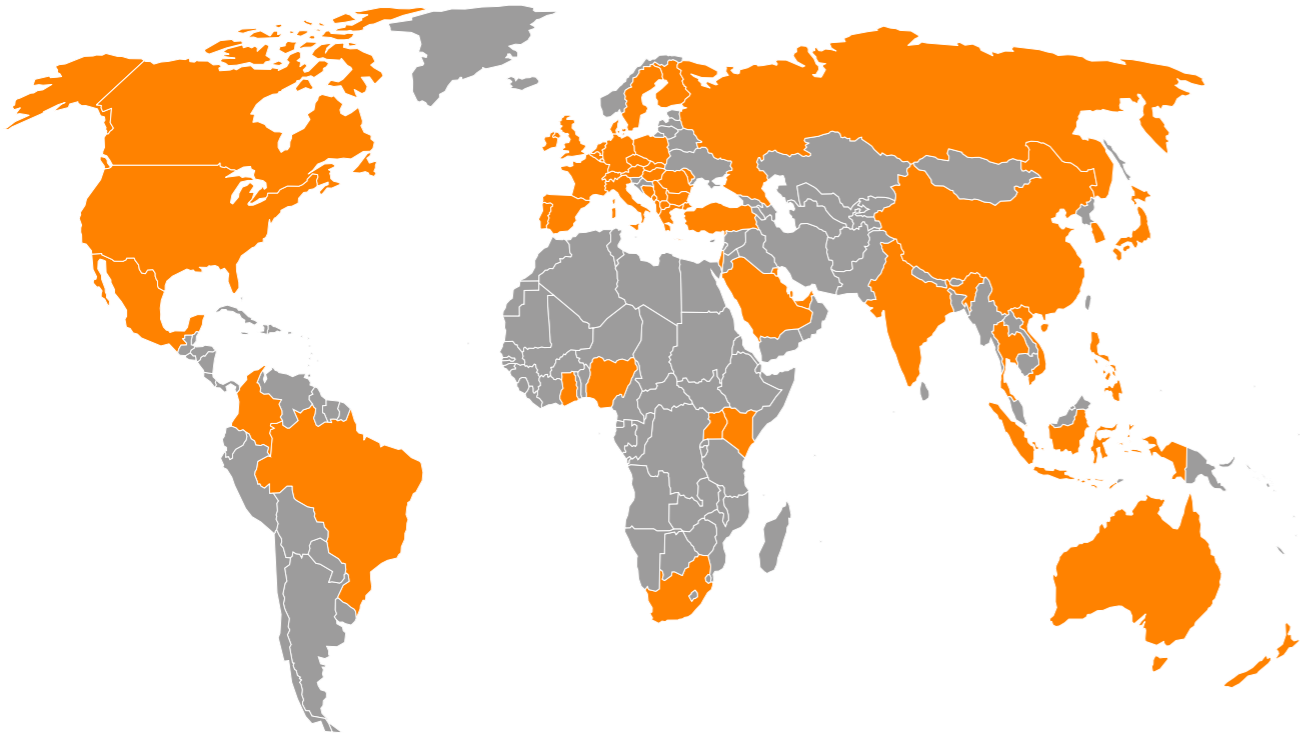
ICTLC è una realtà specializzata e riconosciuta che offre servizi di consulenza multidisciplinare a società ed enti per affrontare al meglio le sfide e le opportunità dell'era digitale.

Il team si avvale delle capacità consulenziali di uno studio legale internazionale - **ICT Legal Consulting** - ed una società di cybersecurity - **ICT Cyber Consulting** - che negli anni hanno acquisito un'esperienza consolidata ed ottenuto significativi risultati con clienti multinazionali nei rispettivi ambiti.



## Le sedi

ICTLC ha sedi in Italia, Olanda, Grecia, Finlandia, Francia, Spagna, Nigeria e Australia e ha stabilito partnership con una molteplicità di studi e professionisti in altri 53 Paesi. Questo ci permette di assistere quotidianamente i nostri clienti in tutto il mondo e di scalare la nostra organizzazione a seconda delle esigenze, mettendo a disposizione i professionisti più adeguati.



### Milano

Via Borgonuovo, 12  
20121  
Tel: +39 02 84247194

### Roma

Piazza di San Salvatore  
in Lauro, 13 - 00186  
Tel: +39 06 97842491

### Bologna

Via Ugo Bassi, 3  
40121  
Tel: +39 051 272036



### Parigi

11 Boulevard de Sébastopol  
75001 - Francia  
Tel: +33 (0) 6 74 55 43 58



### Melbourne

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



### Amsterdam

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



### Madrid

Calle de Alcalá, 75, 28009  
Spagna  
Tel: +34 91 577 50 20



### Atene

Ippokratous 8, 10679  
Grecia  
Tel: +30 210 3600366



### Helsinki

Huopalahdentie 24, 00350  
Finlandia  
Tel: +358 50 4801292



### Lagos

Aggey House (6th Floor) - 12 Berkeley  
Street, Lagos Island, Lagos, Nigeria  
Tel: +234 8150692572

È inoltre presente, **attraverso studi professionali associati**, in altri cinquantatré Paesi: Albania, Arabia Saudita, Austria, Bahrain, Bangladesh, Belgio, Bosnia-Erzegovina, Brasile, Bulgaria, Canada, Cina, Colombia, Corea del Sud, Danimarca, Emirati Arabi Uniti, Filippine, Germania, Ghana, Giordania, India, Indonesia, Irlanda, Israele, Giappone, Kenya, Kuwait, Lussemburgo, Macedonia del Nord, Messico, Moldavia, Montenegro, Nuova Zelanda, Norvegia, Pakistan, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Romania, Russia, Serbia, Singapore, Slovacchia, Stati Uniti, Sudafrica, Svezia, Svizzera, Taiwan, Thailandia, Turchia, Uganda, Ungheria, Vietnam.

# ICT LEGAL CONSULTING



**VI AIUTIAMO A GESTIRE AL MEGLIO E VALORIZZARE I VOSTRI DATI ANCHE NELLE SITUAZIONI PIÙ DIFFICILI.**

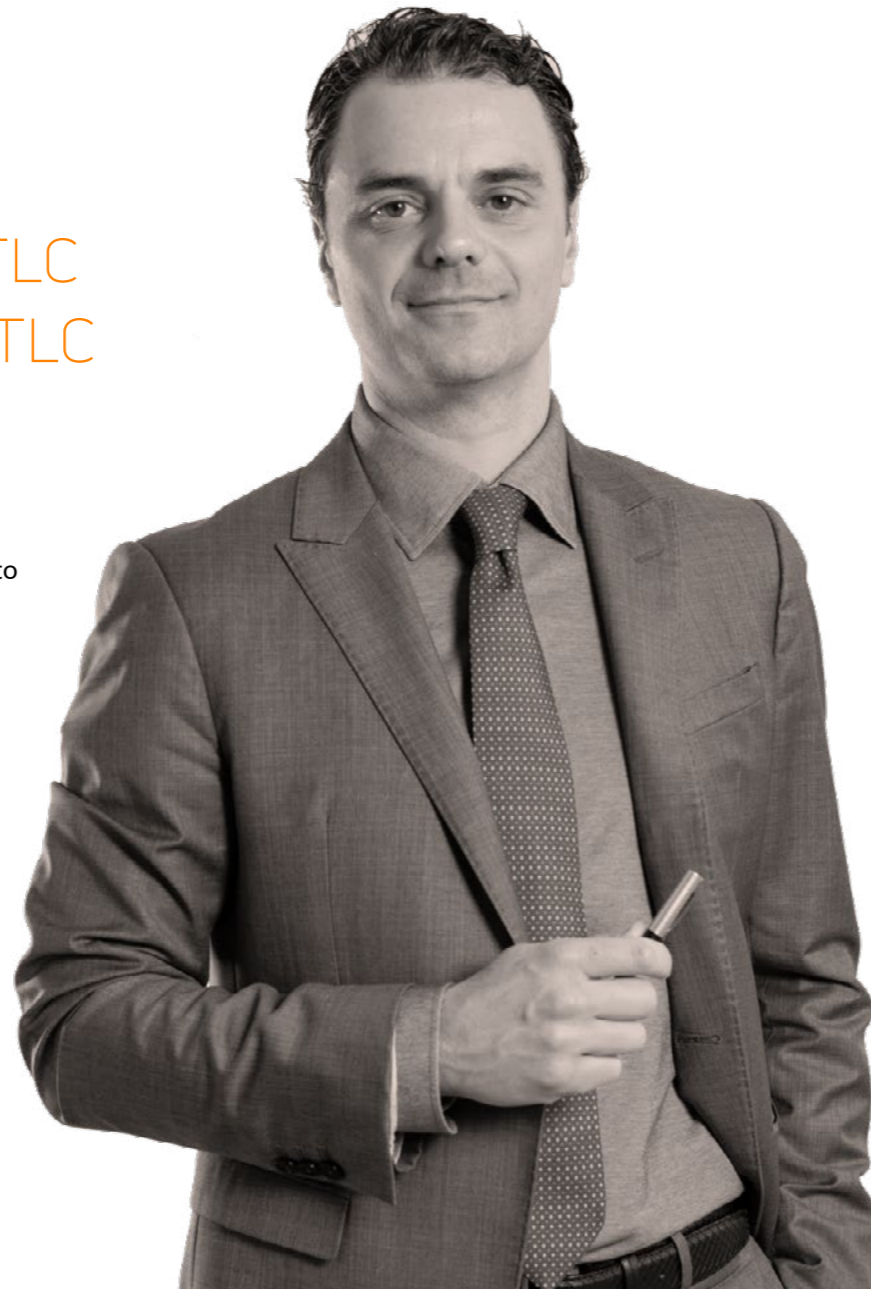
ICT Legal Consulting è uno studio legale internazionale fondato nel 2011 con sedi a **Milano, Bologna, Roma, Amsterdam, Atene, Helsinki, Madrid, Parigi, Lagos e Melbourne.**

È stato creato 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 e della proprietà intellettuale.

## Paolo Balboni

Founding Partner ICTLC  
Managing Partner ICTLC  
International

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 50 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.

## Luca Bolognini

### Founding Partner ICTLC

Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP) dal 2008. Avvocato cassazionista del foro di Roma, è dal 2011 socio fondatore dello studio ICT Legal Consulting con sedi a Milano, Roma, Bologna, Amsterdam, Atene, Helsinki, Madrid, Parigi, Lagos, Melbourne e studi corrispondenti in altri 53 Paesi. Leading Individual Data Privacy and Data Protection The Legal 500 (Italy) 2020-2021-2022-2023. Recommended Lawyer The Legal 500 EMEA 2016-2023. Chambers Europe Ranked Lawyer 2022-2023. IAPP Member, CIPP/E e TÜV Italia Certified Privacy Officer. Socio fondatore di ICTLC S.p.A. e della società di consulenza cybersecurity ICT Cyber Consulting Srl. Laureato in Giurisprudenza all'Alma Mater Studiorum Università di Bologna. Parla fluentemente inglese.



Ha ricoperto e continua a rivestire il ruolo di **ethics & privacy advisor per diversi progetti di ricerca e innovazione europei "Horizon 2020", oltre che di PM board member dei progetti EU H2020 «Privacy Flag», «Cloudwatch 2», «Cyberwatching», «ANITA», «NgIoT», «PREVENT», «NioVe», «PolicyCloud»** ed è, inoltre, attivo come expert coach per l'Executive Agency for Small & Medium-sized Enterprises (EASME) della Commissione Europea. Luca è membro dell'Experts Board di EU-IoT, co-chair della Conferenza internazionale annuale Privacy Symposium di Venezia, co-chair dell'International Board of Senior Experts dello schema di certificazione EuroPrivacy e membro del Comitato dei Saggi dell'Associazione Nazionale per Operatori Responsabili della Conservazione Digitale. Nel 2017 è stato fondatore, con l'Istituto Privacy, del **CNAC - Centro Nazionale Anti-Cyberbullismo**, sostenuto da grandi imprese e importanti studi legali italiani e stranieri. Ha presentato studi e tenuto relazioni in conferenze italiane ed estere (fra le quali CPDP, Annual Privacy Forum, **Privacy Day Forum** e, in più occasioni, **ITU Telecom World**) e pubblicato numerosi articoli su quotidiani e riviste nazionali e internazionali (tra cui The Wall Street Journal, Computer Law & Security Review, Diritto Economia e Tecnologie della Privacy, Il Sole 24 Ore), in materia di protezione dei dati e altri aspetti del diritto, riguardanti ambiti come Intelligenza Artificiale, legal design, Internet delle Cose e Industria 4.0, uso secondario e valorizzazione dei dati, partenariati pubblico-privati data-driven, "class action" privacy, disciplina e-Privacy, Big Data, cloud & edge computing, marketing, sanità e finanza digitali, smart contract, commercio elettronico, sicurezza pubblica digitale, controlli a distanza sul lavoro, responsabilità civile da trattamento di dati, trasferimenti di dati all'estero, libertà di espressione, dati dei minori.

Ha insegnato dal 2010 al 2019 alla **SSPL della Facoltà di Giurisprudenza dell'Università di Teramo** e, dal 2015 al 2018, business data law nel Master in Big Data Management della LUISS Business School;

dal 2016 è docente del Master Unitelma Sapienza "I Professionisti della digitalizzazione e della privacy", in particolare in materia di privacy e lavoro; negli ultimi dieci anni, ha insegnato diritto dei dati e della privacy anche al Master di secondo livello in cybersecurity, data protection and privacy dell'**Università di Roma Tor Vergata**, al Master di secondo livello in Studi Avanzati di diritto del lavoro, organizzazione e relazioni industriali dell'Unimercatorum, al Master in Intelligenza Artificiale, Diritto ed Etica Delle Tecnologie Emergenti dell'Università Europea di Roma, al Master in Data Protection Officer del Politecnico di Milano, al Master in Internet Ecosystem dell'Università di Pisa, all'Advanced Master in Privacy, Cybersecurity and Data Management della Maastricht University, al Master in Ricerca clinica, open innovation e market access nell'era digitale dell'Università Campus BioMedico di Roma, al Master in Advanced Studies on the IoT dell'Università di Ginevra, al Master of Science in Medical Informatics della FHNW University of Applied Sciences and Arts Northwestern Switzerland, al "Corso Maestro Protezione Dati & Data Protection Designer®" dell'Academy Istituto Italiano per la Privacy e ai corsi per Data Protection Officer del **CNR Pisa** e dell'**Università Statale di Milano**. Da anni è regolarmente, inoltre, docente in corsi di alta formazione in materia di diritto dei dati (Master per la Certificazione Privacy Officer TÜV, AFGE, Paradigma, Optime, Scuola Superiore PA, Euroconference, Giuffrè Francis Lefebvre e altri).

Tra i libri di cui è stato autore, co-autore o curatore negli ultimi 15 anni: **"Deontologia Privacy per avvocati e investigatori privati"** (curato con Diego Fulco, Giuffrè, 2009), **"Next Privacy - Il futuro dei nostri dati nell'era digitale"** (curato con Diego Fulco e Pietro Paganini, RCS Etas, 2010), "Privacy Officer" (Ipsa, 2013), "Privacy Technologies and Policies" (Springer, 2016). Co-autore del volume best seller giuridico "Il Regolamento Privacy Europeo" (Giuffrè, 2016), il primo commentario completo italiano al GDPR. Co-autore del volume «Internet of Things Security and Data Protection» (Springer 2019), e in

particolare dei saggi "Evolution of Data Protection Norms and Their Impact on the Internet of Things", "Voluntary Compliance Commitment Tool for European General Data Protection Regulation", "IoT and Cloud Computing: Specific Security and Data Protection Issues". Autore dei pamphlet **"Generazione Selfie"** (Corriere della Sera, 2014) e **"Follia Artificiale - Riflessioni per la resistenza dell'intelligenza umana"** (Rubbettino, 2018), dedicato al rapporto tra diritti umani, ambiente digitale e scenari di intelligenza artificiale. Autore del saggio "La responsabilità civile nel trattamento di dati personali e per atti di cybercrime" parte del trattato «Responsabilità civile dei professionisti e degli altri imprenditori» (Giuffrè, 2018). Co-autore con Enrico Pelino di «Codice Privacy: tutte le novità del D.Lgs. 101/2018» (Giuffrè Francis Lefebvre, 2018). Co-autore con Marco Emanuele Carpenelli del saggio «Larappresentanza dei diritti in materia di protezione dei dati personali, tra azioni plurisoggettive e azioni collettive» nel libro "Azione di classe: la riforma italiana e le prospettive europee" (Giappichelli, 2020). È suo il saggio su trasparenza, accesso ai dati e privacy sanitaria nel trattato «Responsabilità, rischio e danno in sanità» (Giuffrè Francis Lefebvre, 2022). Direttore, con Enrico Pelino, e co-autore dell'estesa opera **«Codice della Disciplina Privacy»** (Giuffrè Francis Lefebvre, 2019-2022), commentario completo al GDPR, al Codice Privacy e a tutte le vigenti normative italiane, primarie e secondarie, in materia di diritto dei dati personali (tra cui il D.Lgs. 51/2018 sui trattamenti di dati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, il D.Lgs. 65/2018 Cybersecurity NIS, e tutti i Provvedimenti generali del Garante Privacy). Curatore e autore del volume «Privacy e libero mercato digitale» (Giuffrè Francis Lefebvre, maggio 2021). Autore de **«L'Arte della Privacy - Metafore sulla (non) conformità alle regole nell'era data-driven»** (Rubbettino, 2022). Autore del libro **«Diritto Dipinto - L'arte legale nel "tutto digitale"»** (Rubbettino, 2023). Alcuni degli open access paper di Luca Bolognini disponibili qui: <https://independent.academia.edu/LucaBolognini1>.



# I NOSTRI SERVIZI

Una combinazione di  
servizi strategici integrati  
in ambito legale e di  
cybersecurity



## Un punto di riferimento unico per tutte le esigenze relative alla gestione strategica della sicurezza dei **dati**.

Supportiamo i nostri clienti in tutto il data "lifecycle": dalla corretta raccolta dei dati fino alla cancellazione dei medesimi. Da un lato, un trattamento in chiave strategica di valorizzazione dei medesimi nel massimo allineamento alla normativa è cruciale per rimanere competitivi sul mercato. Dall'altro, la protezione dei dati e una corretta gestione degli incidenti (**data breach**) al fine di limitarne gli effetti negativi sulle persone e sul business risulta fondamentale per conservare la fiducia di clienti e business partner, assicurando il mantenimento della **brand reputation**. Offriamo un approccio olistico ai nostri clienti, non limitandoci a fornire supporto su questioni legali e sull'implementazione dei workflow concordati, ma anche su come comunicare i risultati raggiunti all'interno e all'esterno dell'organizzazione nel costante sforzo di migliorare la competitività sul mercato e generare un tangibile ritorno sull'investimento (ROI).



Privacy e protezione dei dati personali



Data breach management



Marketing & Digital Advertising



Cloud/Edge/Quantum computing



Artificial Intelligence, Big Data & Smart Analytics



Diritto del lavoro, compliance 231, anticorruzione



E- & M-commerce



Internet of Things



Information & (Tele-) Communication Technology



Blockchain



Proprietà intellettuale/ industriale



e-Health

## Privacy e protezione dei dati personali



- Gap analysis rispetto alla normativa applicabile di data protection e cybersecurity.
- Definizione e manutenzione del sistema di gestione privacy e cybersecurity.
- Supporto ai clienti nella valutazione e gestione di data breach.
- Redazione di contratti per la gestione e valorizzazione dei dati personali.
- Supporto nello sviluppo e nel processo di approvazione delle norme Vincolanti d'Impresa Binding Corporate Rules (BCRs), nonché di contratti di trasferimento dati Standard Contractual.
- Clauses e Transfer Impact Assessment - Supporto nello sviluppo e nel processo di approvazione di Codici di Condotta in materia di protezione dei dati personali (ex art. 40 GDPR).
- Svolgimento del ruolo di data protection office(r).
- Gestione di procedimenti dinanzi ad autorità garanti in materia di privacy.
- Gestione di contenziosi giudiziari inerenti a privacy e protezione dei dati personali.
- Svolgimento di attività di auditing e simulazione di attività ispettive.
- Conduzione di valutazioni d'impatto privacy (DPIA).
- Assistenza nella gestione degli aspetti di privacy e data protection connessi a processi di fusione e acquisizione.

## Cloud/Edge/Quantum computing



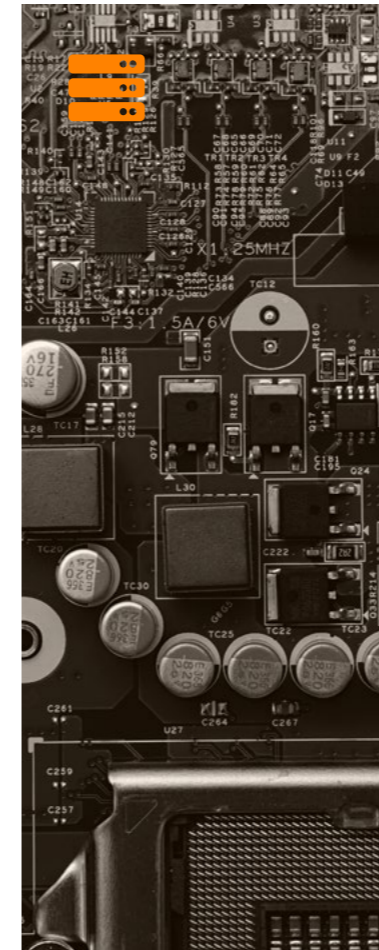
- Redazione di Cloud Computing Service Agreement, SLAs, PLAs e Acceptable Use Policy.
- Supporto in negoziazioni di contratti per la fornitura di servizi cloud Privacy.
- Redazione e negoziazione di Data Processing Agreement per servizi cloud.
- Valutazioni d'impatto (DPIA) su servizi di cloud/edge/quantum computing.
- Transfer Impact Assessment.
- Supporto su problematiche legali e opportunità di migrazione ai servizi cloud (portabilità dei dati).
- Supporto legale sulla selezione del fornitore e del modello cloud da adottare.
- Audit per valutare la conformità di specifici servizi cloud alla normativa in materia di protezione dei dati personali e a standard internazionali di cybersecurity.
- Corsi di formazione sugli aspetti contrattuali e in materia di protezione dei dati personali relativi ai servizi cloud.

## E-&M commerce



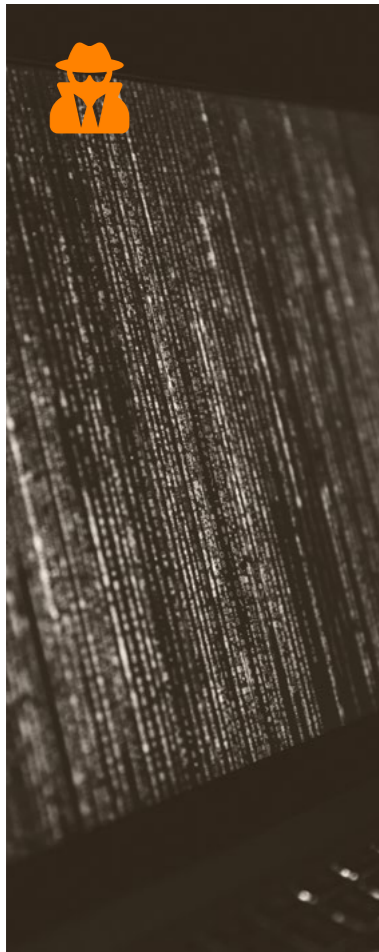
- Legal Impact Assessment di piattaforme di e-commerce e di mobile-commerce, nonché di applicazioni di pagamento.
- Predisposizione di termini e condizioni di vendita/licenza online.
- Valutazione di impatto sulla protezione dei dati (DPIA).
- Transfer Impact Assessment su soluzioni di e- e m-commerce.
- Supporto legale sulla creazione, analisi e la valorizzazione di (grandi) banche dati.
- Predisposizione della documentazione legale necessaria in materia di protezione dei dati personali con riferimento a servizi di E- & M- commerce.
- Assistenza nella negoziazione di contratti di outsourcing con fornitori di servizi di e- e m-commerce.
- Gestione degli aspetti legali e di compliance inerenti alle attività di online advertising/digital marketing (es. programmatic adv).
- Audit per valutare la conformità dei servizi di commercio elettronico (es. condizioni generali, privacy policy e valutazione legale e tecnica delle misure organizzative e di sicurezza delle relative piattaforme e applicativi).
- Consulenza sulla conformità alla normativa dei sistemi di pagamento online.
- Consulenza legale sulla gestione dei contenuti.
- Consulenza legale sui temi inerenti la tutela online dei consumatori, antitrust e concorrenza sleale, proprietà intellettuale/industriale.

## Blockchain



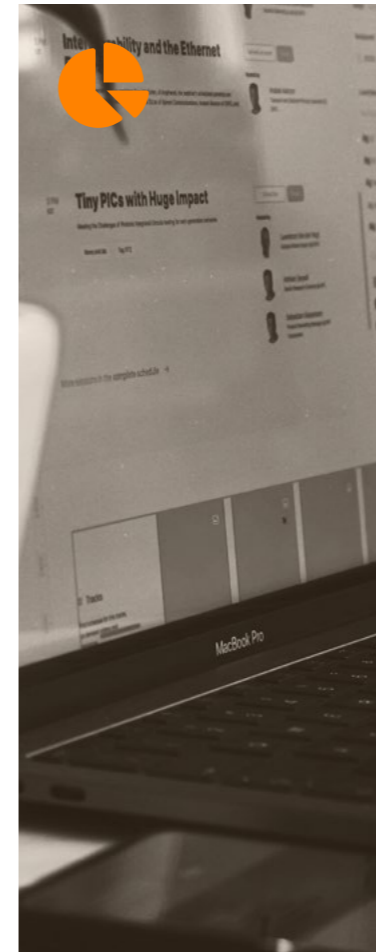
- Information & (Tele-)Communication Technology.
- Supporto legale e tecnico per l'identificazione dei requisiti normativi relativi ad appalti, fornitura e sviluppo di sistemi e servizi di di Information & (Tele-) Communication Technology (Legal Impact Assessment).
- Supporto legale alla conformità con la normativa sulle telecomunicazioni europea ed italiana. Supporto legale sui compiti e gli adempimenti dei fornitori di comunicazioni elettroniche.
- Assistenza nell'interlocuzione con pubbliche autorità ed enti di regolazione.
- Redazione e negoziazione di contratti per lo sviluppo e commercializzazione di servizi di Information & (Tele-)Communication Technology.
- Supporto legale e tecnico su progetti di outsourcing e managed services.
- Supporto legale sullo sviluppo e la distribuzione di software.
- Supporto legale in materia di sviluppo, hosting, gestione dei contenuti e gestione della sicurezza di siti e piattaforme web desktop e mobile.
- Consulenza legale sulla fornitura di servizi di sicurezza (sistemi di videosorveglianza, biometria, antivirus, servizi di backup).
- Audit per valutare la conformità alle normative di settore applicabili.
- Redazione e negoziazione di Service Level Agreement.
- Supporto legale in risoluzioni stragiudiziali e giudiziali delle controversie in materia di Information & (Tele-)Communication Technology.
- Supporto in controversie di fronte all'AGCOM.
- Compliance legale e opportunità di business sulla conservazione dei dati di traffico.
- Supporto legale e opportunità di business legate all'utilizzo di call center

## Cybersecurity



- Valutazioni di impatto legali e tecniche sulla protezione dei dati.
- Consulenza legale e tecnica sugli obblighi inerenti la violazione dei dati in settori regolati come per es. settore sanitario, bancario, fornitura di comunicazioni elettroniche accessibili al pubblico, etc. Sviluppo di policy e documentazione connessa sulla sicurezza delle informazioni.
- Definizione degli aspetti legali inerenti agli aspetti di corporate governance connessi alla sicurezza delle informazioni.
- Allineamento con gli standard ISO 27001.
- Penetration test e vulnerability assessment.
- Gestione della contrattualistica attiva e passiva inerente a servizi di sicurezza informatica.
- Gestione degli aspetti di conformità legale inerenti alla normativa NIS e al Perimetro di Sicurezza Nazionale Cibernetica.
- Audit per valutare la conformità tecnica e legale alle normative applicabili.
- Servizi di hosting per la documentazione inerente la compliance legale.
- Corsi di formazione per dipendenti e dirigenti sulla sicurezza.
- Phishing awareness campaign.
- Per svolgere questo tipo di servizi, utilizziamo i professionisti di ICT Cyber Consulting, spin-off dello studio ICTLC – ICT.Legal Consulting che fornisce orientamento, assistenza e servizi qualificati in materia di sicurezza delle informazioni e cybersecurity. Per saperne di più visita [www.ictcyberconsulting.com](http://www.ictcyberconsulting.com).

## Artificial Intelligence, Big Data & Smart Analytics



- Valutazione sulla conformità legale delle tecnologie di analisi e monitoraggio (Legal Impact Assessment).
- Consulenza legale e tecnica su questioni inerenti “smart city” e reti intelligenti.
- Consulenza legale e tecnica su wearable technologies.
- Data Protection Impact Assessment su soluzioni di Artificial Intelligence, Big Data e Smart Analytics.
- Human Right Impact Assessment su soluzioni di Artificial Intelligence.
- Controlli di Fairness by Design, data protection e data security by design su soluzioni di AI, Big Data e Smart Analytics.
- Consulenza legale e tecnica su soluzioni su smart contracts.
- Supporto legale sulla creazione, la gestione e la valorizzazione di grandi banche dati.
- Consulenza legale su progetti di outsourcing e managed services.

## Internet of Things



- Consulenza legale e tecnica su questioni inerenti “smart city” e reti intelligenti.
- Consulenza legale e tecnica nell’ambito di wearable technologies.
- Valutazione d’impatto (Data Protection Impact Assessment) su trattamenti svolti in complessi ambienti IoT.
- Transfer Impact Assessment relativo a possibili trasferimenti di dati in soluzioni IoT.
- Sviluppo di policy e procedure di gestione dei dati in ambienti IoT.
- Contrattualizzazione dei rapporti tra le parti coinvolte in complessi ambienti IoT (es. Data Management).
- Agreement, Joint-Controllership Agreement.
- Supporto legale sulla creazione, la gestione e la valorizzazione di grandi banche dati.
- Consulenza sulla portabilità dei dati in ambienti IoT.
- Contratti di servizio e condizioni generali.

## Proprietà intellettuale/industriale



- Consulenza stragiudiziale e giudiziale in ogni ambito IP (copyright, segni distintivi, mobile app, disegni e modelli, banche dati, brevetti, concorrenza sleale e pratiche commerciali scorrette, diritto della pubblicità, media&entertainment).
- Contrattualistica IP (ad es. licenze, implementazione di piattaforme e-commerce, franchising e distribuzione selettiva, digital advertising, distribuzione di contenuti audiovisivi).
- Implementazione di nuove tecnologie nel settore IP (IA, blockchain, smart contracts ecc.).
- Assistenza e consulenza in fase pre-contenziosa (ad es. diffide, monitoraggio social media) e contenziosa cautelare, di merito ed esecutiva.
- Gestione del portafoglio IP e consulenza strategica (ad es. IP due diligence, branding, e-commerce), inclusa assistenza nel deposito di domande di registrazione di titoli IP.
- Compliance aziendale (d.lgs 231/2001) e tutela IP.
- Consulenza e assistenza nella tutela degli asset IP in vista dell’implementazione di piattaforme e-commerce e contrattualistica per marketplace.
- Assistenza nella redazione di contratti di sviluppo di siti web, piattaforme e-commerce, mobile apps.
- Protezione del know-how e dei segreti commerciali.
- Gestione dei rapporti con autorità pubbliche (ad es. società di gestione dei diritti d’autore, autorità doganali, uffici nazionali marchi e brevetti, registration authorities).

## Marketing & Digital Advertising



- Valutazioni di compliance legale (Legal Impact Assessment) in materia di protezione dei dati personali e tutela dei consumatori su operazioni di marketing e digital advertising.
- Redazione di informative e privacy policy a supporto di operazioni di marketing e digital advertising.
- Redazione e negoziazione di accordi per operazioni di marketing e digital advertising (es. Data Management Agreement, Joint-Controllership Agreement, etc.).
- Valutazioni d'impatto (Data Protection Impact Assessment) su soluzioni di marketing automation e digital advertising (es. programmatic).
- Due diligence su basi dati di terze parti per lo svolgimento di azioni di marketing.
- Supporto legale regolatorio e in materia di protezione dei dati personali per svolgere manifestazioni a premio nazionali e internazionali.
- Corsi di formazione per dipendenti e dirigenti sulla protezione dei dati personali inerenti le attività di marketing e digital advertising.

## e-Health



- Consulenza legale sulla protezione e sulla sicurezza dei dati sanitari.
- Svolgimento di valutazioni d'impatto (Data Protection Impact Assessment) su soluzioni di e- e mobile-health.
- Supporto legale e tecnico circa la corretta implementazione di soluzioni di Patient Relationship Management (PRM).
- Supporto legale e tecnico per la conformità di dossier sanitari e fascicoli sanitari elettronici.
- Supporto legale e tecnico per la corretta strutturazione di soluzioni di refertazione online.
- Supporto legale e tecnico per la corretta strutturazione di soluzioni di prenotazione online di esami medici.
- Consulenza legale in materia di progetti IT in outsourcing e cloud computing nel settore sanitario.
- Supporto legale e tecnico per offrire soluzioni di telemedicina in conformità alla normativa applicabile.
- Supporto legale sulla gestione dei dati sensibili su dispositivi mobile e indossabili.
- Corsi di formazione in protezione dei dati per dipendenti e dirigenti nel settore sanitario.

## Information & (Tele-) Communication Technology



- Valutazione sulla conformità legale (Legal Impact Assessment) inerenti l'applicazione di tecnologie di blockchain a specifici settori (es. FinTech, InsuranceTech, etc.).
- Valutazioni circa gli aspetti in materia di protezione dei dati personali (Data Protection Impact Assessment) e sicurezza delle informazioni (Data Security Impact Assessment) di soluzioni di blockchain.
- Consulenza legale e tecnica su soluzioni su smart contracts.
- Assistenza in eventuali attività regolatorie (permitting) circa l'utilizzo di soluzioni di blockchain.
- Redazione e negoziazione di contratti attivi e passivi per il deployment di tecnologia blockchain.
- Valutazione e supporto nella operazionalizzazione di tecnologia blockchain per la tutela dei diritti di proprietà intellettuale/ industriale.

## Diritto del lavoro, compliance 231, anti-corruzione



- Assistenza e redazione contratti (anche quadro) nei rapporti società di somministrazione.
- Assistenza nei rapporti sindacali in tema di licenziamenti collettivi- accordi collettivi smart working-videosorveglianza.
- Gestione contenziosi.
- Predisposizione e manutenzione di modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001.
- Consulenza inerente a sistemi di gestione dell'anticorruzione ai sensi dello standard ISO 37001.
- Implementazione di piattaforme e sistemi di whistleblowing.
- Partecipazione quale membro esterno all'organismo di vigilanza nominato ai sensi del D.Lgs. 231/2001.
- Consulenza in favore di enti pubblici relativa all'applicazione della normativa in materia di trasparenza e prevenzione della corruzione, in linea con le linee guida ANAC.

# ICT CYBER CONSULTING

“

CYBERSECURITY E DATA  
PROTECTION BY DESIGN?  
LASCIATE FARE A NOI...

ICT Cyber Consulting è  
una società specializzata  
in **servizi di cybersecurity  
e data protection by  
design tecnologica.**

---

ICT Cyber Consulting nasce nel 2018 come spin-off dello studio  
ICTLC - ICT Legal Consulting con l'obiettivo di offrire soluzioni  
personalizzate che proteggano le aziende.

I nostri esperti sono in grado di offrire una vasta gamma di servizi,  
conoscenza specifica all'avanguardia e completa imparzialità di  
giudizio per ottenere risultati allo stato dell'arte.



## Un punto di riferimento per tutte le esigenze relative alla gestione strategica della sicurezza dei **dati**.

I nostri servizi di consulenza e assistenza perseguono non solo la compliance alle normative e agli standard internazionali, ma anche, e soprattutto, la filosofia del miglioramento continuo. Il PDCA (Plan, Do, Check, Act) conosciuto anche come **Ciclo di Deming** è una metodologia universalmente riconosciuta per la gestione ottimale dei processi aziendali ed è utilizzata come matrice degli standard internazionali ISO in maniera tale da assicurare un miglioramento costante e duraturo. ICTCC crede che lo scenario odierno, caratterizzato da un rapido e costante avanzamento delle nuove tecnologie e delle normative confacenti alla tutela dei dati e delle informazioni debba incontrare un **approccio dinamico e caratterizzato da implementazioni tecniche e organizzative efficaci e personalizzate al contesto aziendale**.



NIS, DORA and PSNC Gap Analysis & Compliance Action Plan



Data Protection Impact Assessment – Cybersecurity



Vulnerability Assessment e Penetration Test



Cybersecurity Gap Analysis



Allineamento Cybersecurity GDPR



Hotline Cybersecurity & Data Breach Management Unit



Valutazione cybersecurity degli applicativi

ISO

ISO/IEC 27001:2013, ISO 22301:2019, ISO 37001:2019, ISO 9001:2015



Privacy by Design



Security Assessment Fornitori Esterni



Audit di seconda parte GDPR, 27001, 22301, 37001



Cybersecurity Awareness

## NIS, DORA and Perimetro Gap Analysis & Compliance Action Plan



Direttiva NIS e D. Lgs. 65/2018 (NISD), Digital Resilience Operational Act (DORA) e Perimetro di Sicurezza Nazionale Cibernetico (PSNC) Gap Analysis & Compliance Action Plan

- Gap Analysis rispetto ai requisiti previsti da NIS, DORA e PSNC
- Metodologia proprietaria di risk assessment: oggettivizzazione del processo di analisi come richiesto dalle linee guida di emanazione ministeriale
- Analisi dello stato dell'arte con dettagli specifici dei gap tra le attuali disposizioni e i requisiti della normativa in conformità con la nostra metodologia e le linee guida tecnica dell'ENISA e del Ministero
- Redazione di un piano d'azione con focus su livello di effort della gestione interna
- Assistenza nella redazione del "Documento da compilare per la mappatura delle misure tecniche e organizzative di sicurezza"
- Progetto operativo volto a risolvere e colmare eventuali lacune in base alle linee guida ENISA e Ministeriali
- Predisposizione delle procedure relative alla gestione degli incidenti di sicurezza e ulteriori misure necessarie alla conformità
- Predisposizione delle procedure relative alla business continuity e al disaster recovery, come richiesto dalle normative
- Valutazione dell'adeguatezza dei fornitori in merito agli aspetti di sicurezza informatica e business continuity, come richiesto dalle normative

## Cybersecurity Gap Analysis



Propedeutica per l'allineamento all'art. 32 GDPR (prima analisi e successive analisi periodiche di aggiornamento)

- Gap analysis propedeutica per allineamento ex art. 32 GDPR "adeguate misure di sicurezza";
- Definizione del perimetro aziendale;
- Verifica della presenza di misure di sicurezza tecniche e organizzative;
- Security risk assessment;
- Redazione di un report puntuale, un documento di riferimento in caso di ispezioni e audit;
- Attività propedeutica per intraprendere processi di certificazione sulla sicurezza informatica aziendale.

## Allineamento Cybersecurity GDPR

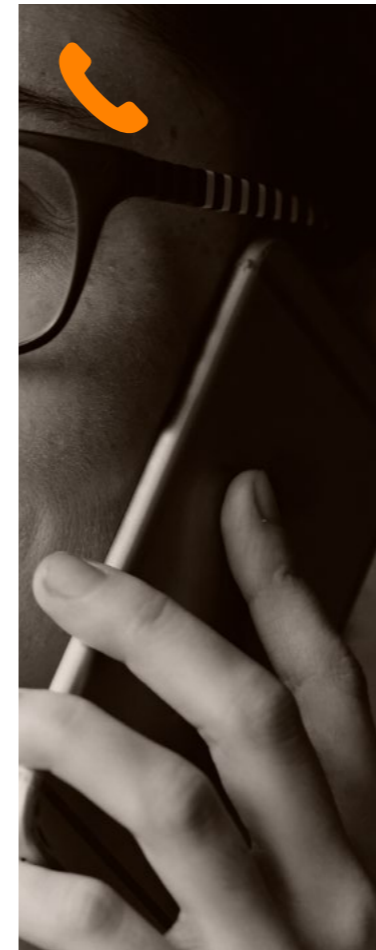


Allineamento cybersecurity all'art. 32 Reg. 2016/679/UE (GDPR)

Una volta individuati i punti di miglioramento aziendali attraverso attività come la Gap Analysis, è comunque necessario creare **processi per l'implementazione di misure tecniche, per la valutazione dei fornitori già contrattualizzati e quelli da contrattualizzare, nonché per la stesura di policy e procedure interne per regolare i business process** e il corretto trattamento dei dati personali.

- Revisione delle liste degli amministratori di sistema, rendendole compatibili con il provvedimento del Garante Privacy del 27 novembre 2008 e successive modifiche;
- **Redazione delle procedure per la valutazione dell'operato degli amministratori di sistema**, in maniera conforme al suddetto provvedimento, o esecuzione della stessa attività, che viene inoltre verbalizzata;
- **Redazione delle procedure per la gestione degli incidenti di sicurezza** e l'eventuale notifica dei data breach, ex artt. 33 e 34 GDPR;
- **Revisione della Policy Strumenti IT** o altra documentazione riguardante l'uso accettabile della strumentazione aziendale;
- Impostazione e redazione di eventuale altra documentazione relativa alla cybersecurity;
- **Assistenza nella predisposizione di tecnologie e procedure per facilitare i diritti dell'interessato** (ad es. nel caso di diritto alla portabilità ex art. 20.1 GDPR e del diritto all'oblio ex art. 17.2 GDPR);
- **Assistenza nell'applicazione e proceduralizzazione del principio di Data Protection by Design/Default** nella progettazione di nuovi processi, prodotti e servizi, a norma dell'art. 25 GDPR.

## Hotline Cybersecurity & Data Breach Management Unit



**Consulenza e assistenza continuativa per la risoluzione delle svariate problematiche cybersecurity, sia via telefono, sia attraverso e-mail**, sia visitando la struttura aziendale ove necessario, per tutta la durata dell'incarico.

In particolare, si prevedono, a titolo esemplificativo, le seguenti attività:

- **Supporto nell'analizzare l'attacco o l'intrusione** in corso, aiutando inoltre nel delineare una strategia di mitigazione rispetto alla minaccia;
- Analisi dei sistemi coinvolti, del traffico di rete, del vettore utilizzato per l'intrusione, della verifica di attacchi, exploit, o payload noti utilizzati per l'intrusione;
- Supporto nell'adozione delle azioni necessarie per la risoluzione del problema, quali ad esempio isolamento delle macchine all'interno della rete, patching o ripristino delle macchine ed esclusione dell'attaccante dalla rete aziendale;
- **Valutazione di prodotti di terze parti** (firewall, SIEM, file integrity monitoring...) da inserire all'interno dell'infrastruttura o già inseriti;
- **Supporto nella progettazione e realizzazione di nuovi prodotti, applicazioni o servizi, mantenendo un elevato livello di sicurezza e secondo i principi di Data Protection by Design e by Default di cui all'art. 25 GDPR**, nonché secondo il Considerando 78;
- **Redazione di un report e/o verbale al termine delle singole attività.**

## Data Protection Impact Assessment – Cybersecurity



La **Valutazione d’Impatto Privacy (DPIA - Data Protection Impact Assessment)** viene effettuata per quei trattamenti di dati che presentano rischi specifici per i diritti degli interessati (cfr. Art. 35 GDPR).

- Predisposizione di un **Modello** basato sulle Guidelines on Data Protection Impact Assessment reperibili all’indirizzo [ec.europa.eu/newsroom/article29/item-detail.cfm](https://ec.europa.eu/newsroom/article29/item-detail.cfm);
- Predisposizione della procedura per i DPIA;
- **Valutazioni sui trattamenti ritenuti a rischio;**
- Delineamento dei rischi principali derivanti da trattamenti ritenuti a rischio e valutazione tramite una metodologia derivante dallo standard ISO/IEC 27005:2018;
- In caso di rischi medioalti, definizione di ulteriori misure di sicurezza atte a mitigarli fino a un livello accettabile.

## Valutazione cybersecurity degli applicativi



Le applicazioni spesso risultano essere il mezzo principale per il trattamento dei dati personali all’interno dell’azienda, ed è quindi opportuno che, durante il processo aziendale di allineamento a GDPR, anch’esse siano sottoposte ad una verifica delle misure di sicurezza in atto, mediante un’adeguata checklist di stato dell’arte.

- **Censimento di tutte le applicazioni ad impatto privacy** (ovvero tutte le applicazioni impiegate per il trattamento di dati personali) utilizzate all’interno dell’infrastruttura aziendale e, attraverso interviste o dimostrazioni sulle varie piattaforme;
- Compilazione di una checklist contenente le misure di sicurezza in atto, allo scopo di evidenziare eventuali lacune (‘gap’) all’interno dell’applicazione;
- Analisi allo stato dell’arte della protezione dei dati personali offerti dall’applicazione, secondo le “*Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*” di ENISA (<https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>) e lo standard ISO/IEC 27001:2022;
- Esamina della presenza di *feature* aggiuntive allo scopo di semplificare il riscontro delle richieste degli interessati, come ad esempio il nuovo diritto introdotto da GDPR, ovvero il diritto alla portabilità ex art. 20 GDPR;
- Redazione di un **dettagliato Report**, che includerà la metodologia eseguita al fine di poterla riattuare periodicamente, nonché tutti i gap riscontrati con le relative raccomandazioni allo scopo di incrementare il livello di sicurezza degli applicativi.

**ISO/IEC  
27001:2022, ISO/  
IEC 22301:2019,  
ISO 37001:2019,  
ISO 9001:2015,  
ISO 55001:2014**



La sicurezza informatica sta ricoprendo oggi giorno un ruolo sempre più centrale, soprattutto all'interno delle realtà aziendali. Va da sé che la scelta di un prodotto o di un fornitore non avviene esclusivamente valutando le feature proposte: tra le variabili in gioco nel mercato odierno, oltre al rapporto qualità/prezzo, rientrano anche le **misure di sicurezza messe a disposizione dal fornitore**. È dunque necessario conoscere lo stato dell'arte in materia di cybersecurity per valutare lo stato aziendale in merito e procedere a migliorie.

**Standard ISO/IEC 27001:2022:** information security management system.

**Standard ISO 22301:2019:** business continuity management system.

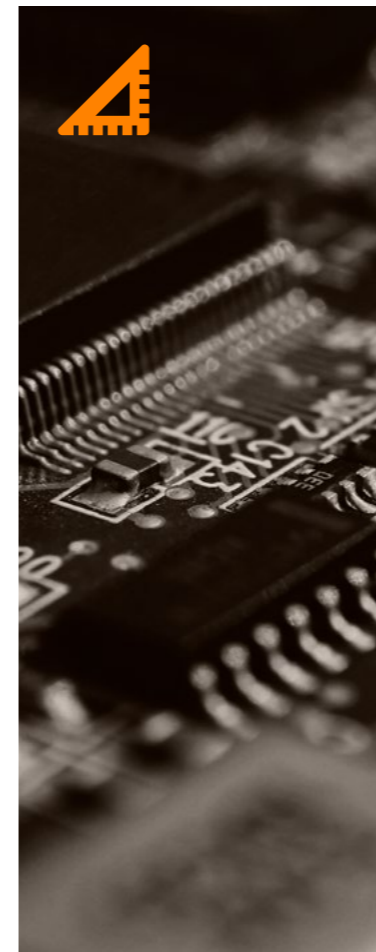
**Standard ISO 37001:2016:** anti-bribery management systems.

**Standard ISO 9001:2015** quality management system.

**Standard ISO 55001:2014:** asset management system.

- Consulenza per l'accompagnamento della vostra organizzazione alla certificazione;
- Analisi dei vari controlli ISO;
- Redazione delle relative policy e procedure;
- Verifica del contesto aziendale;
- Individuazione lacune (gap);
- Selezione degli obiettivi di controllo e attività di controllo per la gestione dei rischi;
- Assunzione del rischio residuo da parte del management;
- Report finale contenente raccomandazioni utili a incrementare il livello di sicurezza aziendale;
- Integrazione e applicazione dei controlli dello standard ISO prescelto con i relativi obblighi legali in materia di protezione dei dati personali.

## Privacy by Design



Una delle innovazioni contenute nel Regolamento (EU) 2016/679 è il principio di **data protection by design and by default**, da applicare a tutti i processi, sistemi e software all'interno dell'infrastruttura aziendale.

- Studio di fattibilità: rendere disponibili le informazioni necessarie alla decisione sull'effettiva realizzazione tecnica di quanto richiesto;
- Valutazione del contesto informatico, dello stato dell'arte di sistemi, applicativi e flussi di informazioni coinvolti;
- Identificazione dei vincoli tecnici;
- Analisi dettagliata delle interrelazioni sistemistiche e delle possibili problematiche che l'attivazione di determinate funzionalità può indurre;
- Valutazione e quantificazione dei rischi relativi alla sicurezza informatica al fine di eliminarli o ridurli;
- Definizione di possibili soluzioni da adottare, definendo nel dettaglio i componenti hardware e software su cui si necessita l'implementazione;
- Guida nell'adozione, implementazione e configurazione delle soluzioni individuate.

## Vulnerability Assessment e Penetration Test

### Vulnerability Assessment

- Analisi di sicurezza dell'infrastruttura IT per identificare potenziali vulnerabilità e fornire misure rimediali per mitigarne i rischi;
- Uso di tool professionali automatizzati;
- Evidenza di problematiche come servizi configurati in modo non sicuro, applicativi obsoleti vulnerabili, sistemi operativi obsoleti, ecc.

### Penetration Testing

- Simulazione di attacco informatico per la valutazione dell'adeguatezza delle misure di sicurezza tecniche e organizzative dell'azienda.

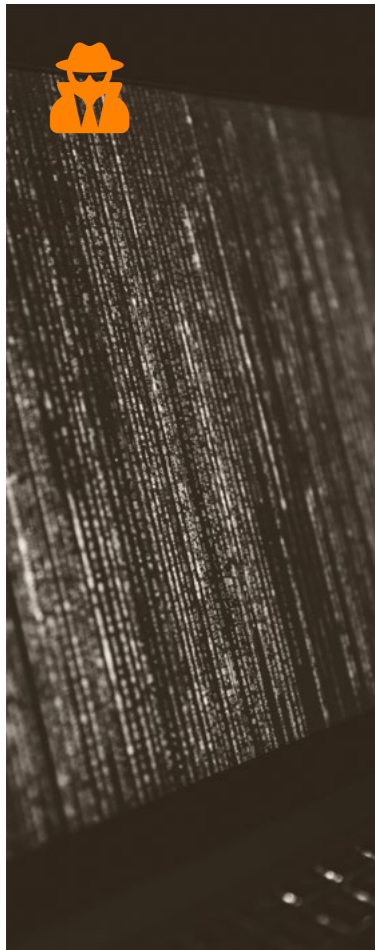
#### Tipologie

- **Penetration test interno**, al tester viene fornito l'accesso alla rete aziendale ed un account di dominio per simulare un attaccante che è riuscito a fare breccia nelle misure di sicurezza perimetrali della vostra azienda;
- **Obiettivo**: verifica della resilienza dell'infrastruttura IT e la possibilità di fare escalation dei privilegi all'interno del dominio aziendale per esfiltrare dati critici per il business aziendale;
- **Penetration test esterno**: simula un vero e proprio attacco informatico con l'obiettivo di fare breccia nell'infrastruttura IT della vostra azienda a partire dai servizi esposti. È possibile svolgere il penetration test esterno nelle metodologie whitebox, greybox e blackbox, che si differenziano per la quantità di informazioni fornite al tester ed al personale dell'azienda.

#### Output

**Executive Summary**: un report breve, con indicazioni di carattere non tecnico utile a comprendere i rischi a cui è esposta l'infrastruttura IT;

**Technical Report**: un report esteso destinato al personale tecnico dell'organizzazione. L'obiettivo del report è esporre in modo completo e chiaro le criticità individuate oltre che fornire anche informazioni su come risolvere tali problematiche.



## Security Assessment fornitori esterni

L'**art. 28** del **GDPR** obbliga il Titolare del trattamento a procedere ad una valutazione dell'adeguatezza al Regolamento per i fornitori che trattano dati personali per nome e conto del Titolare, riguardo gli aspetti di sicurezza informatica.

- Verifica adeguatezza dell'infrastruttura tecnica e organizzativa del fornitore in relazione al **provvedimento del Garante Privacy del 27 novembre 2008**;
- Verifica adeguatezza dell'infrastruttura tecnica e organizzativa del fornitore in relazione alle **Technical Guidelines for the implementation of minimum security measures for Digital Service Providers** dell'ENISA.



## Audit di seconda parte GDPR, 27001, 22301, 37001, 55001

Audit di seconda parte per la valutazione della **compliance** del modello tecnico e organizzativo vigente alle norme e ai principali standard internazionali

- Data Protection (GDPR);
- **ISO/IEC 27001:2022**: information security management system;
- **ISO 22301:2019**: business continuity management system;
- **ISO 37001:2016**: anti-bribery management system,
- **ISO 55001:2014**: asset management system.



## Cybersecurity awareness



### Corsi di formazione

In presenza, tramite webinar e a distanza in materia di data protection, cybersecurity e sistemi di gestione. Mettiamo a disposizione un Learning Management System (LMS) di proprietà, piattaforma applicative online semplice e intuitiva, con funzionalità avanzate ed alto contenimento dei costi dei corsi:

- Rilascio certificato individuale al superamento dei moduli;
- Facile monitoraggio centralizzato dei risultati;
- Alta personalizzazione della formazione a seconda delle esigenze dell'azienda.

### Simulazioni di Attacco Phishing

Phishing Assessment: esecuzione di tentativi di phishing tramite tecniche di ethical hacking volte a testare la consapevolezza di tali attacchi all'interno dell'organizzazione.

- Metodologia proprietaria, consolidata e altamente personalizzabile sulle specifiche del target.
- Monitoraggio del comportamento di ciascun utente.
- Indicazioni temporali sulle azioni compiute dai destinatari delle e-mail.
- Tracciamento degli eventi come apertura e-mail, click sul link malevolo, inserimento di credenziali, ecc.

Output

**Executive Summary:** report rivolto al top management, con indicazioni di carattere non tecnico ed esplicita individuazione sintetica delle risultanze

**Activity Report:** report esteso, destinato al personale tecnico, con dettagli completi delle attività condotte, specifica della metodologia seguita, trattamento particolareggiato delle risultanze e descrizione completa delle possibili azioni correttive.

## Consulenza strategica nei principali settori produttivi

L'interesse per le tematiche di cui ci occupiamo è alla base della passione che ci porta ad eccellere nella nostra professione attraverso massimo impegno e cura per i dettagli.



Istruzione



Energia



Banking & Finance



Assicurazioni



Life science



Sport, Media & Entertainment



Food & Beverage



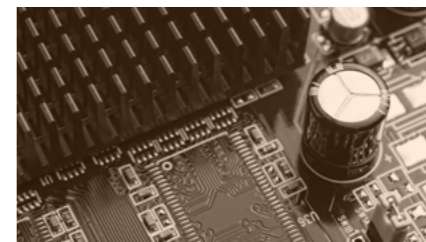
Appalti pubblici



Hospitality & Leisure



Retail




Tecnologia



Healthcare



The background of the image is a composite of two photographs of Earth from space. The upper portion shows the bright, orange-gold glow of the sun rising over the horizon, creating a lens flare effect. The lower portion shows the Earth at night, with a dark blue atmosphere and numerous bright yellow and white lights from cities and towns, indicating a high-latitude or high-altitude perspective.

**Eccellenza** nei risultati, **passione**  
per ciò che facciamo e **flessibilità**  
nel servire i nostri clienti sono le  
pietre miliari del successo di ICTLC.



---

**ICTLC ITALIA**

Via Borgonuovo, 12 - Milano

**Business:**

[info@ictlc.com](mailto:info@ictlc.com)

**Amministrazione:**

[admin@ictlc.com](mailto:admin@ictlc.com)

**P. Iva:**

IT11711660966

**PEC:**

[ictlc@pec.it](mailto:ictlc@pec.it)

**Web:**

[www.ictlc.com](http://www.ictlc.com)

---

