



ICTLC

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



SUMMARY

THE GROUP	04
OFFICES	06
THE LAW FIRM	08
LEGAL SERVICES	16
ICT CYBER CONSULTING	30
CYBER SERVICES	32
INDUSTRIES	46

THE GROUP

ICTLC

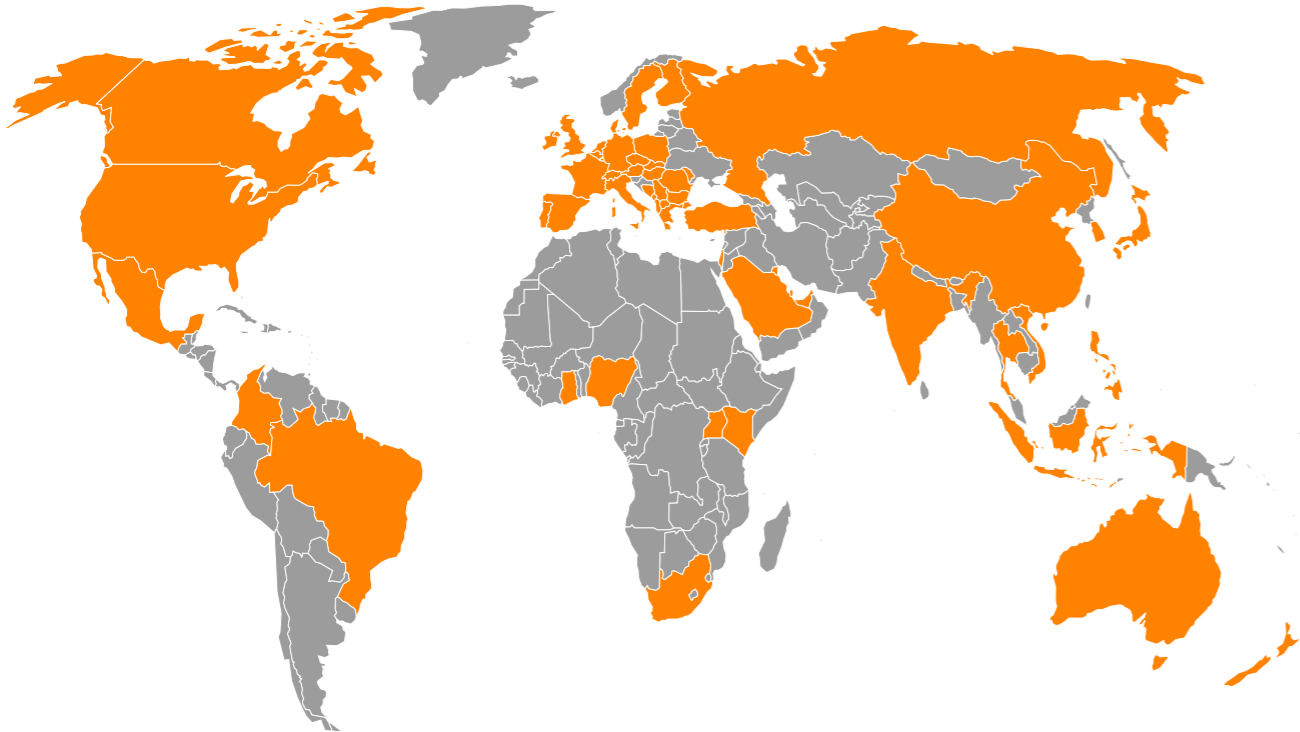
ICTLC is an International Group that offers strategic support in legal compliance (Privacy, IP, TMT) and assists in drafting and developing governance, organisation, management, security and control models for your data-driven organization.

Our team combines the expertise of two realities which are already established on the international market, **ICT Legal Consulting** – an international law firm – and **ICT Cyber Consulting** – a cybersecurity consulting company. Over the years, both companies have acquired significant experience and obtained demonstrable results in their respective fields, consolidating a close-knit team of over 80 qualified professionals.



Offices

In each of these countries we have established partnerships with more than one law firm.
 According to the project, we contact the most qualified professionals who are most suited to the specific needs of our clients.



Milan
 Via Borgonuovo, 12
 20121 - Italy
 Tel: +39 02 84247194



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

Rome
 Piazza di San Salvatore
 in Lauro, 13 – 00186 - Italy
 Tel: +39 06 9138 5512



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

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



Athens
 Ippokratous 8, 10679
 Greece
 Tel: +30 210 3600366



Paris
 11 Boulevard de Sébastopol
 75001 – France
 Tel: +33 (0) 6 74 55 43 58



Helsinki
 Huopalahdentie 24, 00350
 Finland
 Tel: +358 50 4801292



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



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

The firm is **present in fifty-three other countries**: Albania, Austria, Bangladesh, Bahrain, Belgium, Bosnia & Herzegovina, Brazil, Bulgaria, Canada, China, Colombia, Czech Republic, Denmark, Germany, Ghana, Hungary, India, Indonesia, Ireland, Israel, Japan, Jordan, Kenya, Kuwait, Luxembourg, Mexico, Moldova, Montenegro, New Zealand, North Macedonia, Norway, Pakistan, Philippines, Poland, Portugal, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, Uganda, UK, USA, Vietnam.

THE LAW FIRM



ICT Legal Consulting is an international law firm founded in 2011 with offices in **Milan, Bologna, Rome, Amsterdam, Athens, Helsinki, Madrid, Paris, Lagos and Melbourne.**

The firm was established by Paolo Balboni and Luca Bolognini, who have successfully assembled a network of trusted, highly skilled lawyers specialized in the fields of Information and Communication Technology, Privacy, Data Protection/Security, and Intellectual Property Law. ICTLC has offices in Italy, the Netherlands, Greece, Finland, France, Spain, Nigeria and Australia and has established partnerships with law firms and professionals in **53** other countries. This allows us to assist our clients around the world on a daily basis while also scaling our organization to provide the local legal advice our clients' businesses require.

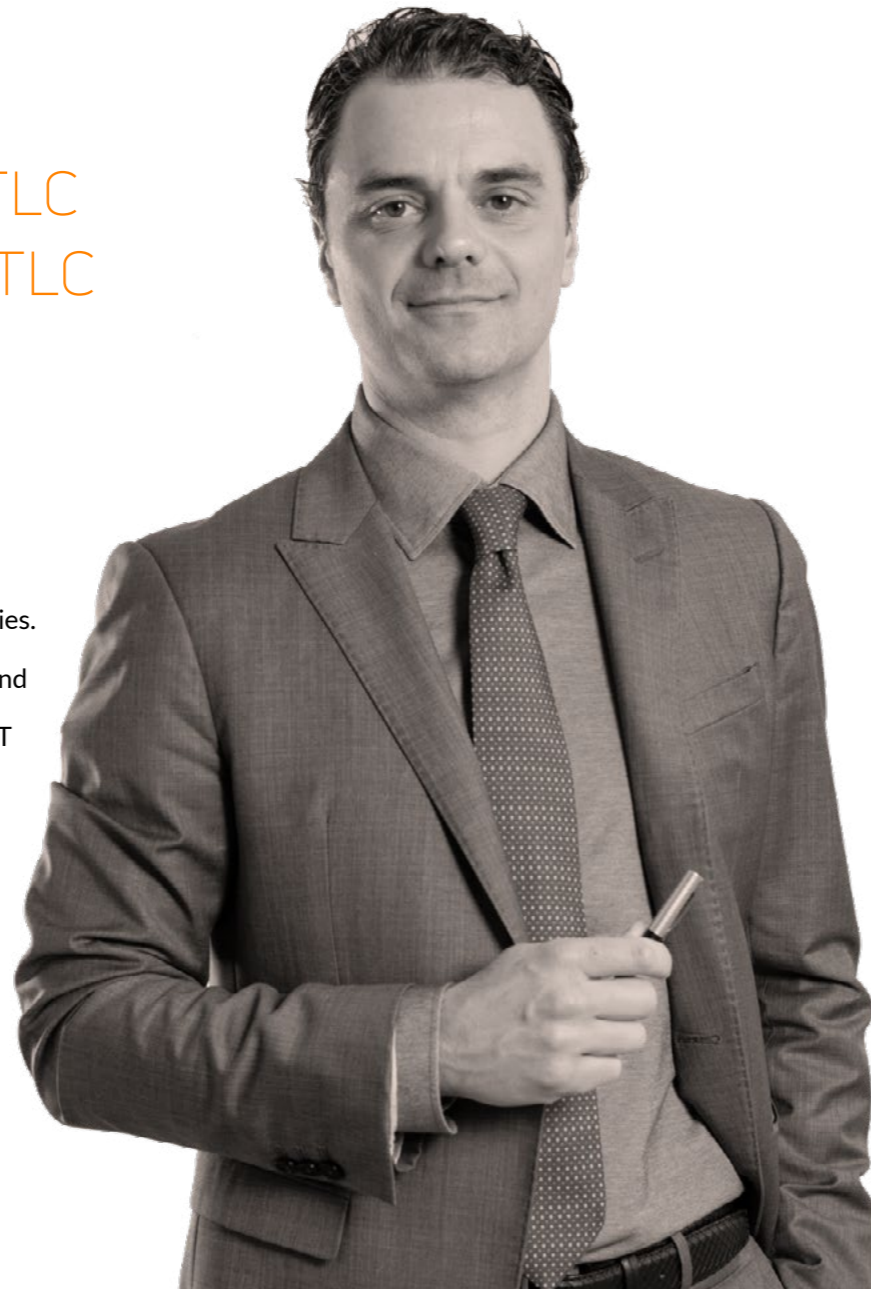


**DATA LIES
AT THE CENTER
OF OUR SERVICES**

Paolo Balboni

Founding Partner ICTLC
Managing Partner ICTLC
International

Paolo Balboni (Ph.D.) is a top tier European ICT, Privacy & Cybersecurity lawyer and serves as Data Protection Officer (DPO) for multinational companies. He is a qualified lawyer admitted to the Milan Bar and the Amsterdam Bar and is a Founding Partner of ICT Legal Consulting (ICTLC), an international law firm with offices in Milan, Rome, Bologna, Amsterdam, Madrid, Athens, Helsinki, Paris, Lagos and Melbourne, and partner law firms in more than 50 countries around the world. He is a Founder 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.

Paolo Balboni is also Professor of Privacy, Cybersecurity, and IT Contract Law at the [European Centre on Privacy and Cybersecurity](#) (ECPC) within the Maastricht University Faculty of Law. He is Chairman of the [European Patent Office](#) (EPO) Data Protection Board, Member of the [EUMETSAT](#)

Data Protection Supervisory Authority, Member of the [Europrivacy Board of Experts](#), and Member of the European Commission's [Expert Group on B2B data sharing and cloud computing contracts](#).

Paolo is Co-Chair of the Cloud Security Alliance [Privacy Level Agreement](#) (PLA). Recommended Lawyer ranked by The Legal 500 EMEA 2023 in the areas of Data Privacy and Data Protection and Industry Focus: TMT.

Paolo 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. Paolo furthermore advises the Dutch government on national matters concerning cybersecurity and privacy and in 2018 drafted the national Surinamese Privacy and Data Protection Law.

Keynote speaker at numerous international conferences on the legal aspects of Cybersecurity, ICT contracts, Privacy & Data

Protection matters; Paolo 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 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.

* Prof. Dr. Paolo Balboni has registered the following principal (and secondary) legal practice areas in the Netherlands Bar's register of legal practice areas (in Dutch: "rechtsgebiedenregister"): Privacy Law, Information Law (IT-Law), and Intellectual Property Law. Based on this registration, he is required to obtain ten training credits per calendar year in each registered principal legal practice area in accordance with the standards set by the Netherlands Bar.

Luca Bolognini

Founding Partner ICTLC

President of the Italian Institute for Privacy and Data Valorisation (Istituto Italiano per la Privacy e la Valorizzazione dei Dati), since 2008.

Luca is an attorney-at-law admitted to practice before the Italian Supreme Court, a member of the Rome Bar Association and founding partner of the law firm ICT Legal Consulting with offices in Milan, Rome, Bologna, Amsterdam, Athens, Helsinki, Madrid, Paris, Lagos, Melbourne and partner law firms in 53 other countries.

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 and TÜV Italia Certified Privacy Officer.

Co-founder and shareholder of the data compliance consulting firm ICTLC SpA and of the cybersecurity firm ICT Cyber Consulting Srl. He obtained his Law degree from the Alma Mater University of Bologna.



Luca serves as an independent **Ethics and Privacy Advisor for several European research and innovation projects (Horizon 2020 / Horizon Europe)** and as an Expert Coach for the Executive Agency for Small & Medium-sized Enterprises (EASME) of the European Commission. Member of the PM boards of the EU H2020 projects "Privacy Flag", "Cloudwatch 2", "Cyberwatching", "ANITA", "NGIoT", "PREVENT", "NiOVe", "PolicyCloud". In 2017, he founded the **"CNAC - National Center Anti-Cyberbullying"**, supported by relevant Italian and international companies and law firms. He speaks Italian and English fluently and has reasonable knowledge of Spanish. He has published studies on data protection and other legal aspects concerning Artificial Intelligence, e-Privacy, secondary use of data in the scientific research, R&D and marketing fields, Big Data, international data transfers, cloud & edge computing, Internet of Things and Industry 4.0, smart contracts, fintech, e-health, data processing liability and privacy "class actions", right to monetize data, freedom of information, right to be forgotten, minors' privacy, profiling, and pseudonymization for scientific journals and both national and international newspapers (including Computer Law & Security Review, Diritto Economia e Tecnologie della Privacy, Corriere della Sera, Sole 24 Ore, Il Mondo, Affari Italiani, European Voice, The Wall Street Journal).

Luca is co-founder of the Privacy Symposium International Conference in Venice. He is a member of the Experts Board of **EU-IoT** and **co-chair of the EuroPrivacy Certification Scheme Board of Senior Experts**. He regularly participates as a speaker to national and international conferences (including ITU Telecom World, IoT Week, Annual Privacy Forum, Privacy Day Forum, CPDP) and radio/TV broadcasts on innovation policies matters. He has lectured at Alma Graduate School of the University of Bologna, Scuola Superiore della Pubblica Amministrazione, **CNR Pisa**, **Università**

Statale di Milano, IED, IPSOA and TÜV Sud Privacy Officer mastercourses and at several other training and higher education programs and masters in Italy. From 2010 to 2019, he has been in charge of teaching privacy law at the SSPL at the Faculty of Law of the University of Teramo, Italy. In the last 10 years, Luca's been in charge of teaching EU data protection law at the Master in Big Data Management of LUISS Guido Carli, at the 2nd level Master in cybersecurity, data protection and privacy at the **University of Rome Tor Vergata**, at the 2nd level Master in Labour Law at the Unimercuratorum, at the 2nd Level Master in Data Protection Officer at Politecnico di Milano, at the 1st level Master in Professionisti della digitalizzazione e della privacy at the University Unitelma Sapienza, at the 1st level Master in Intelligenza Artificiale, Diritto ed Etica Delle Tecnologie Emergenti at the Università Europea di Roma, at the "Corso Maestro Protezione Dati & Data Protection Designer®" at the Academy Istituto Italiano Privacy, at the Master in Internet Ecosystem at the University of Pisa at the Advanced Master in Privacy, Cybersecurity and Data Management at Maastricht University, at the Master of Science in Medical Informatics at FHNW University and at the Master in Advanced Studies on the IoT at the **University of Geneva**.

Luca Bolognini's books in the last 15 years, as editor, author or co-author: "Deontologia privacy per avvocati e investigatori privati" (privacy for lawyers and private investigators, Giuffrè, 2009); "Next Privacy" (RCS Etas, 2010); "Privacy Technologies and Policies" (chapter on IoT and 3D privacy, Springer, 2016); "Generazione Selfie" (Corriere della Sera, 2014); "Il Regolamento Privacy Europeo" (the first Italian commentary on the GDPR, Giuffrè, 2016); "La responsabilità civile nel trattamento di dati personali e per atti di cybercrime" (on personal data processing-related liability, Giuffrè Francis Lefebvre, 2018); "Codice Privacy: tutte

le novità del D.Lgs. 101/2018" (Giuffrè Francis Lefebvre, 2018); "AI. Artificial Insanity - Reflections on the resilience of human intelligence" (Rubbettino, 2018), a pamphlet about digital rights, Big Data law and impacts of Artificial Intelligence, AR/VR and IoT on human lives; "Internet of Things Security and Data Protection" (Springer, 2019), in particular with the essays **"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"; «La rappresentanza dei diritti in materia di protezione dei dati personali, tra azioni plurisoggettive e azioni collettive» in the book "Azione di classe: la riforma italiana e le prospettive europee" (essay on privacy and data protection class actions, Giappichelli, 2020); "Responsabilità, Rischio e Danno in Sanità" (chapter on privacy and data transparency in the Italian health sector, Giuffrè Francis Lefebvre, 2022). Director, with Enrico Pelino, and author of the volume **«Codice della Disciplina Privacy»** (Giuffrè Francis Lefebvre, 2019, 1454 pages), a complete commentary to the GDPR and all the Italian data protection and privacy laws. Editor and author of the book "Privacy e libero mercato digitale" (Giuffrè Francis Lefebvre, 2021), on the balance and interaction between data protection and other sectoral market regulations. Author of the book **«L'Arte della Privacy - Metafore sulla (non) conformità alle regole nell'era data-driven»** (Rubbettino, 2022, English edition: «The Art of Privacy - Metaphors on (non) compliance in the data-driven era», Spanish edition: «El Arte de la Privacidad - Metáforas sobre la (no) conformidad con las reglas en la era de los datos»). Author of the book **«Diritto Dipinto - L'arte legale nel "tutto digitale"»** (Rubbettino, April 2023).

Some of Luca Bolognini's open access papers: <https://independent.academia.edu/LucaBolognini1>.



OUR SERVICES

A combination of
integrated strategic legal
and cybersecurity services

OUR LEGAL SERVICES

A one-stop shop for all **data** management and exploitation needs

Processing data with a view to its enhancement and enrichment in absolute compliance with current regulations is crucial for companies to maintain their competitive advantage. On the other hand, data protection and the proper management of incidents (data breaches) to mitigate any negative impact on people or business, is equally important in preserving the trust of both customers and business partners, as well as ensuring brand reputation.

We adopt a holistic approach in supporting our clients, not only helping them with legal issues and implementing agreed workflows, but also helping them communicate the results achieved both within and outside of their organisations, in a constant effort to improve market competitiveness and generate a tangible return on investment (ROI). The support we offer covers the entire data lifecycle, from collection to deletion.



Privacy
and data protection



Cloud/Edge/Quantum
computing



E- & M-commerce



Blockchain



Cybersecurity



Artificial Intelligence,
Big Data & Smart Analytics



Internet of Things (IoT)



Industrial/Intellectual
Properties



Marketing &
Digital Advertising



e-Health



Information & (Tele-)
Communication Technology



Labor law, 231 compliance,
anti-corruption

Privacy and data protection



- Application gap analysis on data protection and cybersecurity regulations.
- Definition and maintenance of a privacy and cybersecurity management system.
- Client support in data breach assessment and management.
- Personal data enhancement and management contracts.
- Support in developing and approving Binding Corporate Rules (BCRs) and Standard Contractual Clauses.
- Contractual Clauses and Transfer Impact Assessment - Support in developing and approving personal data protection Codes of Conduct (art. 40 GDPR).
- Acting as Data Protection Office(r).
- Management of proceedings before the Data Protection National Supervisory Authorities.
- Management of legal disputes concerning privacy and personal data protection.
- Audits and simulated inspections.
- Data Protection Impact Assessments (DPIA).
- Assistance in managing privacy and data protection aspects associated with mergers and acquisitions.

Cloud/Edge/Quantum computing



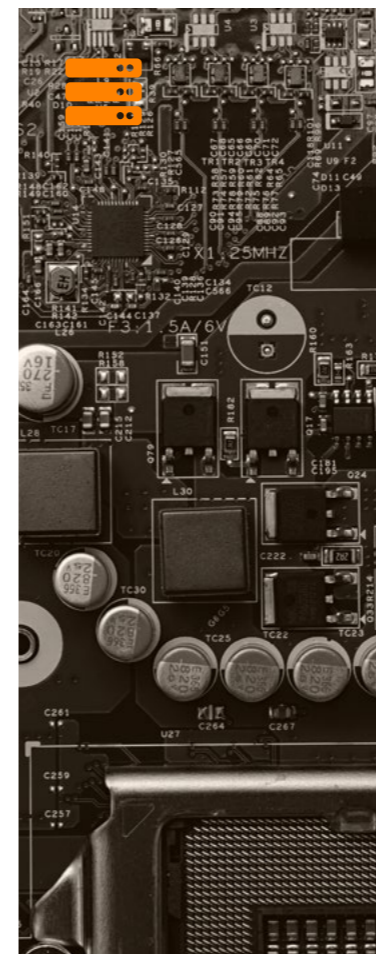
- Cloud Computing Service Agreements, SLAs, PLAs, and Acceptable Use Policy.
- Support in negotiating cloud service provision contracts.
- Drafting and negotiating cloud service Data Processing Agreements.
- Data Protection Impact Assessment (DPIA) on cloud/edge/quantum computing services.
- Transfer Impact Assessment.
- Support on legal issues and opportunities in migration to cloud services (data portability).
- Legal support on vendor selection and cloud model adoption.
- Audits to assess compliance of specific cloud services with data protection regulations and international cybersecurity standards.
- Training on contractual and data protection aspects of cloud services.

E- & M-commerce



- Legal Impact Assessment of e-commerce and mobile-commerce platforms and payment applications.
- Preparation of terms and conditions for online sales/licensing.
- Data Protection Impact Assessment (DPIA).
- Transfer Impact Assessment on E-commerce and M-commerce.
- Legal support on the creation, analysis, and exploitation of (large) databases.
- Preparation of the necessary legal documentation on personal data protection for E-commerce and M-commerce services.
- Assistance in negotiating outsourcing contracts with E-commerce and M-commerce service providers.
- Management of the legal and compliance aspects of online advertising/digital marketing activities (e.g., programmatic advertising).
- Audits to assess the compliance of E-commerce services (e.g., general terms and conditions, privacy policy, legal and technical evaluation of organizational and security measures of related platforms and applications).
- Consulting on the regulatory compliance of online payment systems.
- Legal advice on content management.
- Legal advice related to online consumer protection, Antitrust and unfair competition, intellectual/industrial property.

Blockchain



- Legal Impact Assessment of the application of blockchain technologies to specific sectors (e.g., FinTech, InsuranceTech, etc.).
- Data Protection Impact Assessment (DPIA) and Data Security Impact Assessment of blockchain solutions.
- Legal and technical advice on smart contracts.
- Assistance in regulatory activities (permitting) for the use of blockchain solutions.
- Drafting and negotiating contracts for blockchain technology deployment.
- Evaluation and support in the operationalization of blockchain technology for the protection of intellectual/industrial property rights.

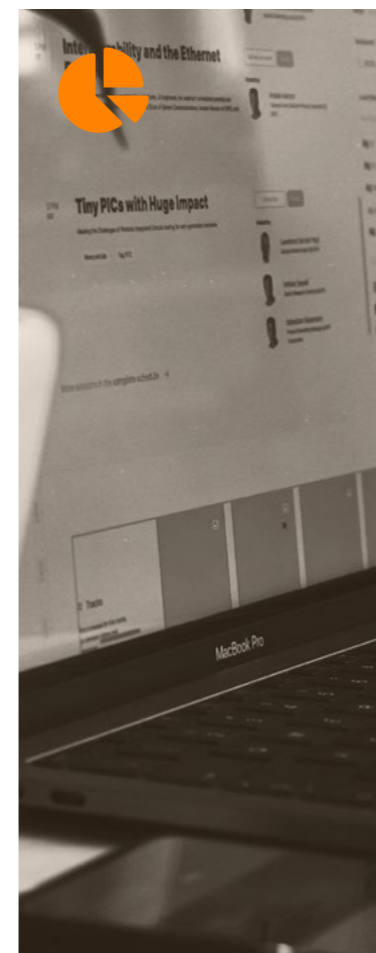
Cyber- security



- Data protection legal and technical impact assessments.
- Legal and technical advice on data breach obligations in regulated industries such as healthcare, banking, publicly accessible electronic communications, etc., development of information security policies and related documentation.
- Definition of the legal aspects of corporate governance related to information security.
- Alignment with ISO 27001 standards.
- Penetration testing and vulnerability assessment.
- Management of active and passive information security services contracts.
- Management of legal compliance aspects in accordance with NIS and the National Cyber Security Perimeter.
- Audits on technical and legal compliance with applicable regulations.
- Hosting services for legal compliance documentation.
- Security training for employees and managers.
- Phishing awareness campaigns.

For these services we rely on the professionals from ICT Cyber Consulting, a spin-off of ICTLC - ICT Legal Consulting, who provide guidance, assistance, and qualified services in the field of information security and cybersecurity. To learn more visit www.ictcyberconsulting.com

Artificial Intelligence, Big Data & Smart Analytics



- Assessment of the legal compliance of analytics and monitoring technologies (Legal Impact Assessment).
- Legal and technical advice on smart cities and smart networks.
- Legal and technical consultancy on wearable technologies.
- Data Protection Impact Assessment on Artificial Intelligence, Big Data, and Smart Analytics solutions.
- Human Rights Impact Assessment on Artificial Intelligence solutions.
- Fairness by Design, data protection, and data security by design on AI, Big Data, and Smart Analytics solutions.
- Legal and technical advice on smart contracts solutions.
- Legal support on the creation, management, and enhancement of large databases.
- Legal advice on outsourcing and managed services projects.

Internet of Things (IoT)



- Legal and technical advice on smart cities and smart networks.
- Legal and technical consultancy on wearable technologies.
- Data Protection Impact Assessment on data processing carried out in complex IoT environments.
- Transfer Impact Assessment on potential data transfers in IoT solutions.
- Development of policies and procedures for data management in IoT environments.
- Contracts to manage relationship between parties involved in complex IoT environments (e.g., Data Management).
- Agreements, Joint-Controllership Agreement.
- Legal support on the establishment, management, and enhancement of large databases.
- Consulting on data portability in IoT environments.
- Service contracts and general conditions.

Industrial/Intellectual Properties



- Extrajudicial and judicial consultancy in every IP context (copyright, distinctive signs, mobile apps, designs and models, databases, patents, unfair competition, and unfair commercial practices, advertising, Media & Entertainment).
- IP contracts (e.g., licenses, implementation of e-commerce platforms, franchising and e-commerce, franchising and selective distribution, digital advertising, distribution of audiovisual content).
- Implementation of new IP sector technologies (AI, blockchain, smart contracts, etc.).
- Assistance and consultancy in pre-litigation (e.g., warning notices, social media monitoring) and precautionary, merit, and executive litigation.
- IP portfolio management and strategic consulting (e.g., IP due diligence, branding, e-commerce), including assistance in filing applications for the registration of IP titles.
- Corporate compliance (Italian Legislative Decree 231/2001) and IP protection.
- Advice and assistance in protecting IP assets when implementing e-commerce platforms and marketplace contracts.
- Assistance in drafting contracts for websites, e-commerce platforms, mobile app development.
- Protection of know-how and trade secrets.
- Management of relations with the public authorities (e.g., copyright management companies, customs authorities, national trademark and patent offices, registration authorities).

Marketing & Digital Advertising



- Legal compliance assessments (Legal Impact Assessment) on personal data and consumer protection in marketing and digital advertising operations.
- Drafting of privacy policies to support marketing and digital advertising operations.
- Drafting and negotiating agreements for marketing and digital advertising operations (e.g., Data Management Agreements, Joint-Controllership Agreements, etc.).
- Data Protection Impact Assessment on marketing automation and digital advertising solutions (e.g., programmatic).
- Due diligence on third-party databases for marketing.
- Regulatory and data protection legal support for participation in national and international competitions.
- Training courses on personal data protection in marketing and digital advertising for employees.

e-Health



- Legal advice on health data protection and security.
- Data Protection Impact Assessments on E- and M-health solutions.
- Legal and technical support on the proper implementation of Patient Relationship Management (PRM) solutions.
- Legal and technical support on the compliance of health dossiers and electronic health records.
- Legal and technical support in developing online reporting solutions.
- Legal and technical support in setting up online booking solutions for medical examinations.
- Legal advice on outsourced IT projects and cloud computing in the healthcare sector.
- Legal and technical support in providing telemedicine solutions under applicable regulations.
- Legal support on the management of sensitive data on mobile and wearable devices.
- Data protection training courses for employees and managers in the healthcare industry.

Information & (Tele-) Communication Technology



- Legal and technical support in identifying regulatory requirements relating to the procurement, supply, and development of Information & (Tele-) Communication Technology (Legal Impact Assessment).
- Legal support for compliance with European and Italian telecommunications regulations and on the tasks and obligations of electronic communication providers.
- Assistance in dealing with public authorities and regulatory bodies.
- Drafting and negotiating contracts for the development and marketing of Information & (Tele-)Communication Technology services.
- Legal and technical support on outsourcing and managed services projects.
- Legal support on software development and distribution.
- Legal support on the development, hosting, content and security management of desktop and mobile websites and platforms.
- Legal advice on the provision of security services (video surveillance systems, biometrics, antivirus, backup services).
- Audits on compliance with applicable industry regulations.
- Drafting and negotiating Service Level Agreements.
- Legal support in the judicial and amicable composition of Information & (Tele-) Communication Technology related disputes.
- Support in disputes before AGCOM.
- Legal compliance and business opportunities related to traffic data retention.
- Legal support and business opportunities related to the use of call centers.

Labor law, 231 compliance, anti-corruption



- Assistance and drafting of contracts (including framework contracts) with staff leasing companies.
- Assistance in union relations on collective employment agreements, smart working, video surveillance.
- Litigation management.
- Preparation and maintenance of Organizational, Management and Control models under Legislative Decree 231/2001.
- Consulting on anti-corruption management systems based on the ISO 37001 Standard.
- Implementation of whistleblowing platforms and systems.
- Participation as an external member of Supervisory Bodies under Legislative Decree 231/2001.
- Consulting for public bodies on the application of transparency and corruption prevention regulations, in line with ANAC guidelines.

ICT CYBER CONSULTING

“

CYBERSECURITY AND DATA
PROTECTION BY DESIGN? DON'T
WORRY, WE'VE GOT YOU COVERED

ICT Cyber Consulting is a firm specialized in **cybersecurity services** and **technological data protection by design.**

ICT Cyber Consulting was established in 2018 as a spin-off from ICT Legal Consulting with the aim of offering customised solutions that keep businesses safe.

Our experts are able to offer a wide range of cybersecurity services, cutting-edge specific knowledge and complete impartiality of judgment to achieve state of the art results.

OUR CYBER SERVICES

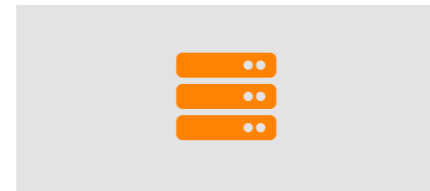
A one-stop shop for all needs related to strategic data security management.

Our services pursue not only compliance with international regulations and standards but also, and above all, the **philosophy of continuous improvement**. PDCA, also known as the **Deming Cycle**, is a universally recognized methodology for the optimal management of business processes and is used as a matrix of international ISO standards to ensure constant and lasting improvement.

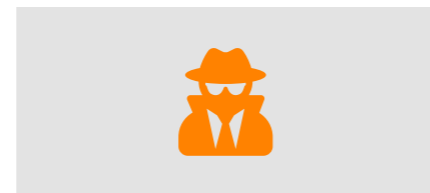
ICTCC believes that today's scenario, which involves a fast and constant advancement of new technologies and regulations regarding the protection of data and information, must be met with a **dynamic approach characterized by effective technical and organizational implementations tailored to the business context**.



NIS, DORA, PSNC Gap Analysis & Compliance Action Plan



Data Protection Impact Assessment – Cybersecurity



Vulnerability Assessment and Penetration Test



Cybersecurity Gap Analysis



GDPR Cybersecurity Alignment



Hotline Cybersecurity & Data Breach Management Unit



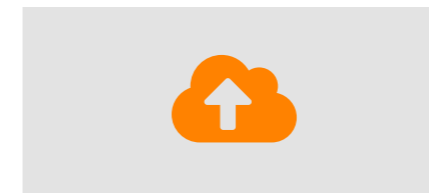
Cybersecurity assessment of applications



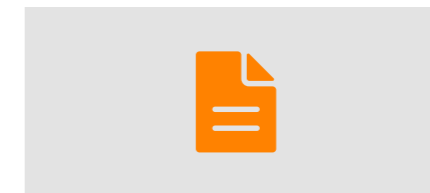
ISO/IEC 27001:2022, ISO 22301:2019, ISO 37001:2019, ISO 9001:2015, ISO 55001:2014



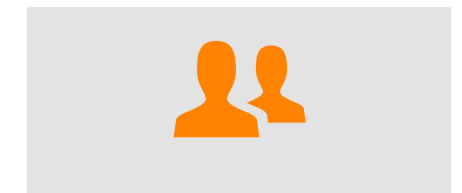
Privacy by Design



Security Assessment External Suppliers



2nd party audits GDPR, 27001, 22301, 37001



Cybersecurity Awareness

NIS, DORA, PSNC Gap Analysis & Compliance Action Plan



NIS Directive, Digital Operational Resilience Act and Regulations regarding the National Cybernetic Security Perimeter Gap Analysis & Compliance Action Plan

- Gap Analysis regarding the provisions of NIS, DORA and Perimetro.
- Proprietary risk assessment methodology: objectification of the analysis process as required by ministerial guidelines.
- Detailed assessment highlighting the gaps between the current provisions and the requirements of the regulations in accordance with our methodology and the technical guidelines of ENISA and the Ministry.
- Drafting of an action plan highlighting the effort of internal management.
- Assistance in drafting the “Document to be completed for mapping technical and organizational security measures”.
- Operational project to address and fill any existing gaps based on ENISA and Ministerial guidelines.
- Drafting of procedures with respect to security incident management and additional measures necessary for compliance.
- Drafting a procedure with respect to the business continuity and disaster recovery, as required by the regulations.
- Assessment of the adequacy of the suppliers with regard to IT security and business continuity aspects, as required by the regulations.

Cybersecurity Gap Analysis



Preliminary phase for alignment with Art. 32 GDPR (first analysis and periodic update analyses)

- Gap analysis prior to alignment under Art. 32 GDPR’s adequate security measures;
- Defining the company perimeter;
- Verification of the existence of technical and organizational security measures;
- Security risk assessment;
- Drafting a detailed report, a reference document in case of inspections and audits;
- Preliminary activities to undertake certification processes on corporate IT security.

GDPR Cybersecurity Alignment



Cybersecurity alignment to Art. 32 Reg. 2016/679/EU (GDPR)

As a result of the assessment activity, it is essential to set up processes for implementing technical measures, evaluating current and potential suppliers, and drafting internal policies and procedures to regulate business processes and the proper personal data management.

- Revising the lists of system administrators, aligning them with the measure of the Italian Data Protection Authority of November 27, 2008, as amended;
- Drafting of procedures for evaluating the work of system administrators, according to the aforementioned measure;
- Reviewing the activities of system administrators and drafting a report thereon;
- Drafting of procedures for managing security incidents and possible notification of data breaches, pursuant to Articles 33 and 34 GDPR;
- Reviewing the IT Tools Policy or other documents relating to the acceptable use of company equipment;
- Setup and drafting of any other cybersecurity-related documents;
- Assistance in setting up technologies and procedures to ease the rights of the data subject (e.g., in the case of the right to portability under Article 20.1 GDPR and the right to be forgotten under Article 17.2 GDPR);
- Assistance in the enforcement and formalisation of the Data Protection by Design/Default principle in the design of new processes, products, and services, pursuant to Art. 25 GDPR.

Hotline Cybersecurity & Data Breach Management Unit



Ongoing consultancy and assistance in resolving various cybersecurity issues, either via phone, e-mail, or by visiting the corporate facility when necessary.

Specifically, the following activities, by way of example, are expected:

- Support in investigating the attack or intrusion currently underway, assisting also in strategically outlining a mitigation solution with respect to the threat;
- Analysis of the systems involved, network traffic, the vector used for the intrusion, verifying known attacks, exploits, or payloads used for the intrusion;
- Support in the adoption of necessary actions to address the problem, such as isolating machines within the network, patching or restoring machines, and excluding the attacker from the corporate network;
- Assessment of third-party products (firewall, SIEM, file integrity monitoring...) to be included within the infrastructure or already in use;
- Support in the design and implementation of new products, applications, or services, with a high level of security and per the principles of Data Protection by Design and by Default under Article 25 GDPR, as well as under Recital 78;
- Preparation of a report and/or minutes upon completion of individual activities.

Data Protection Impact Assessment – Cybersecurity



Data Protection Impact Assessment (DPIA) is conducted for those data processing activities that pose specific risks to the rights of data subjects (see Art. 35 GDPR).

- Provision of a Model based on the Guidelines on Data Protection Impact Assessment available at ec.europa.eu/newsroom/article29/item-detail.cfm;
- Provision of the procedure for DPIAs;
- Assessments of processing activities deemed to be at risk;
- Outlining key risks from data processing activities considered to be at risk and assessment using a methodology derived from the ISO/IEC 27005:2018 standard;
- In case of medium-high risks, the definition of additional security measures to mitigate them to an acceptable level.

Cybersecurity assessment of applications



Applications frequently prove to be the primary vehicle for personal data processing in the organization. It is therefore appropriate that during the company's GDPR alignment process, applications are subjected to an evaluation of the security measures in place through evaluation checklists.

- Mapping all privacy-impacting applications (i.e., all applications used to process personal data) used within the corporate infrastructure through interviews or demonstrations on the various platforms;
- Drafting a checklist containing the existing security measures to highlight any gaps within the application;
- Analysis of the protection of personal data offered by the application, according to ENISA's "Technical Guidelines for the implementation of minimum-security measures for Digital Service Providers" (<https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>) and the ISO/IEC 27001:2022 standard;
- Analysis of the existence of additional features to simplify the response to data subjects' requests, such as the new right introduced by GDPR, i.e., the right to portability under Article 20 GDPR;
- Drafting a detailed report, which shall include the methodology performed to re-implement it periodically, as well as all the gaps found with related recommendations to increase the security level of the applications.

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

ISO

Nowadays, IT security is playing an increasingly central role, especially in corporate establishments. Several factors influence the choice of a product or vendor companion: value for money and other market variables aside, security measures are among the paramount factors. Therefore, it is necessary to know the current cybersecurity status to assess the company's condition in this regard and make improvements.

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

ISO 22301:2019 Standard: business continuity management system

ISO 37001:2016 Standard: anti-bribery management system

ISO 9001:2015 Standard: quality management system

ISO 55001:2014 Standard: asset management system

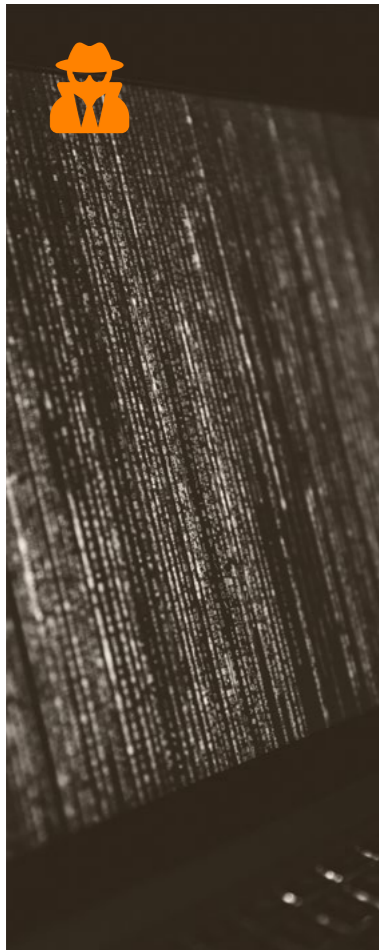
- Guiding your organization to certification;
- Analysis of the relevant ISO controls;
- Drafting of pertinent policies and procedures;
- Audit of the company's business environment;
- Gaps identification;
- Selecting control goals and monitoring activities for risk management;
- Assumption of residual risk by management;
- Final report providing valuable recommendations to increase the level of corporate security;
- Integration and implementation of the controls of the selected ISO standard with the relevant legal obligations on personal data protection.

Privacy by Design

Among the innovations under Regulation (EU) 2016/679 is the principle of data protection by design and by default, to be enforced for all processes, systems, and software within the corporate infrastructure.

- Feasibility assessment: providing the necessary information required to decide on the technical implementation of requirements;
- Assessment of the IT context in terms of systems, applications, and information flows involved;
- Identifying of technical constraints;
- Detailed analysis of system interactions and possible issues connected to the activation of certain functionalities;
- Assessing and quantifying IT security risks in order to remove or reduce them;
- Defining possible solutions to be adopted, outlining in detail the hardware and software components involved;
- Guidance in the adoption, implementation, and configuration of the identified solutions. soluzioni individuate.

Vulnerability Assessment and Penetration Test



Vulnerability Assessment

- Security assessment of the IT infrastructure to identify potential vulnerabilities and provide remedial measures to mitigate the risks;
- Use of professional automated tools;
- Evidence of security issues such as improperly configured services, vulnerable outdated applications, outdated operating systems, etc.

Penetration Testing

Simulated cyber-attack to assess the adequacy of the company's technical and organizational security measures.

Types

- **Internal penetration testing:** the tester has access to the corporate network and a domain account to simulate an attacker who has managed to breach the company's perimeter security measures. The goal of this assessment is to verify the resilience of the IT infrastructure and the ability to perform privilege escalation within the corporate domain to exfiltrate business-critical data.
- **External penetration testing:** simulates an actual cyber-attack aiming at breaching the company's IT infrastructure by exploiting the exposed services. The external PT may be conducted in the white-box, grey-box, or black-box methodologies, which differ in the amount of information provided to the tester and company personnel.

Output

- **Executive Summary:** a short report with non-technical information, useful to understand the risks which may affect the IT Infrastructure;
- **Technical Report:** an extensive report designed for the organization's technical staff. This report aims to fully and clearly expose the critical issues identified and providing information on how to resolve these issues.

Security Assessment external suppliers



Article 28 GDPR requires the Data Controller to conduct an adequacy assessment of the compliance with the Regulation concerning the IT security aspects for suppliers that process personal data on behalf of the Data Controller.

- Verify the adequacy of the provider's technical and organizational infrastructure in relation to the provision of the Italian Data Protection Authority of November 27, 2008;
- Adequacy assessment of the technical and organizational infrastructure of the provider with the "Technical Guidelines for the implementation of minimum-security measures for Digital Service Providers" of ENISA.

2nd party audits GDPR, 27001, 22301, 37001, 55001

Second-party audits to assess the existing technical and organizational model's compliance with regulations and leading international standards.

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



Cybersecurity Awareness

E-learning courses on data protection, cybersecurity, and management systems.

Face-to-face, webinar and distance learning courses on data protection, cybersecurity and governance systems. We provide a proprietary Learning Management System (LMS), a simple and intuitive online application platform with advanced functionalities and high course cost containment:

- Individual certificate issuance upon successful completion of modules;
- Easy centralised monitoring of results;
- High customisation of training according to company needs.

Service of Phishing Attack Simulations

ICT Cyber Consulting's Phishing Assessment activity consists in carrying out phishing attempts through ethical hacking techniques aimed at testing the awareness of such attacks within the organisation. These attempts are carried out using a proprietary, consolidated methodology that can be customised to the specifics of the target system. Through our service, the controller and the processor are able to define a procedure that meets the requirements of Article 32(1)(d) GDPR regarding technical and organisational security measures against attack vectors based on e-mail and on the misuse of the human factor. Our methodology also allows us to define corrective actions that are suitably tailor-made for the organisation.

Through our Phishing Assessment service, we provide detailed information on the events surrounding a phishing campaign. In particular, we are able to monitor the behaviour of each user and also to provide timestamps on the actions of the employees receiving the e-mails.

Output: Executive Summary and Activity Report



Legal & cyber consulting

The interest in what we do is the basis of the passion that drives us to excel in our work and constantly offer commitment and attention to detail.



Education



Energy



Financial services



Insurance



Life science



Media sport and entertainment



Food and beverage



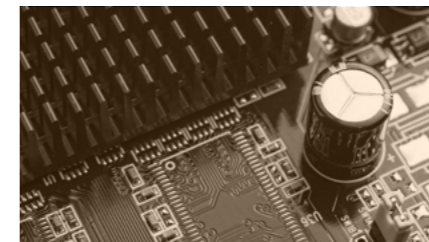
Government contracting



Hospitality and leisure



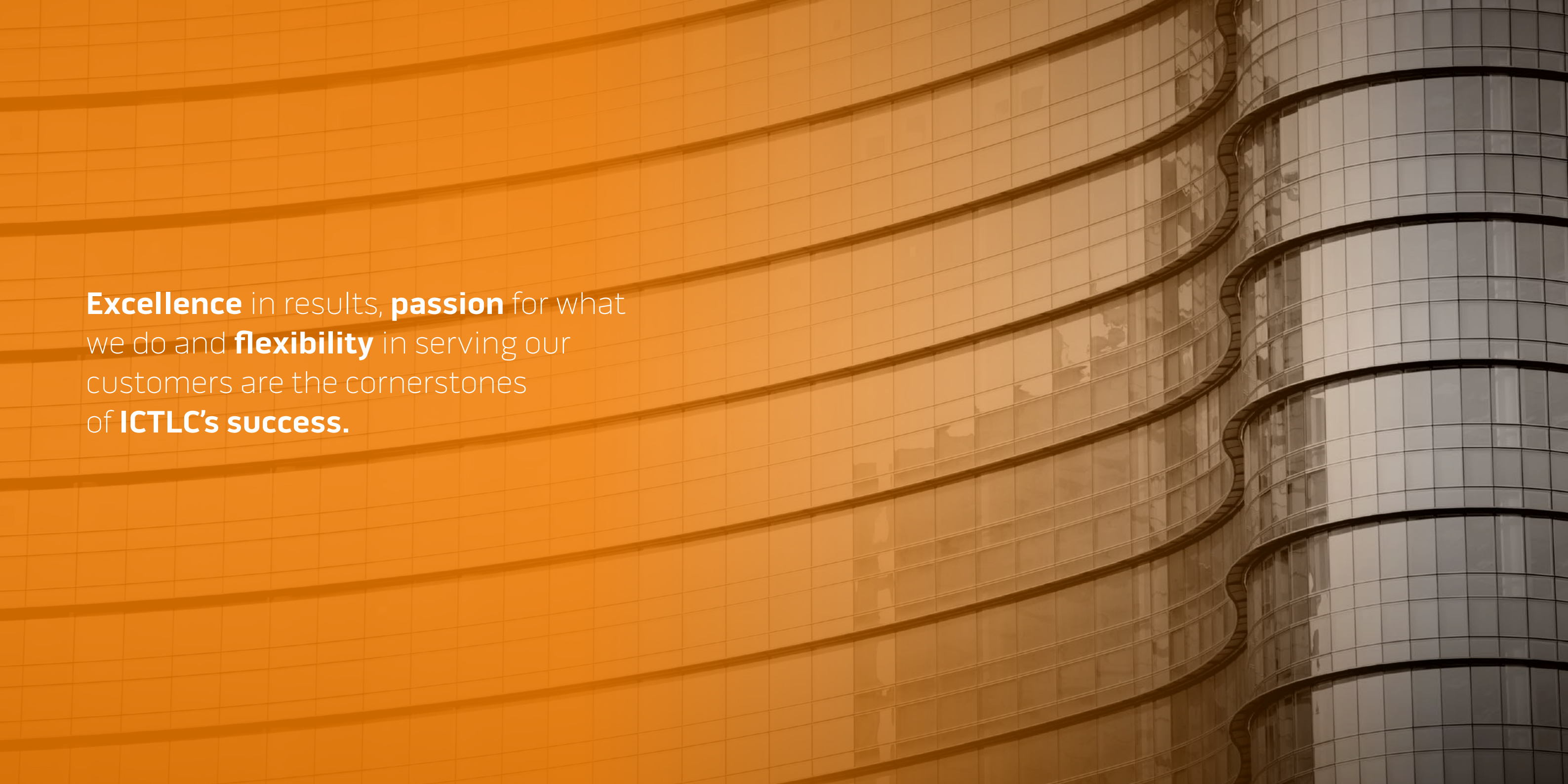
Retail



Technology



Healthcare



Excellence in results, **passion** for what we do and **flexibility** in serving our customers are the cornerstones of **ICTLC's success.**



ICTLC

Via Borgonuovo, 12 - Milan

Business inquiries:

info@ictlc.com

Administration:

admin@ictlc.com

VAT Number:

IT11711660966

PEC:

ictlc@pec.it

Web:

www.ictlc.com

