

# DATA CONSEC

DATA PROTECTION - CONSULTING - SECURITY

Catalogo  
SERVIZI

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

# DATA CONSEC

DATA PROTECTION - CONSULTING - SECURITY

## CHI SIAMO

La missione di DataConSec è quella di costruire insieme ai propri clienti strategie adeguate a proteggere il loro bene più prezioso: le informazioni critiche per il business e i dati personali che essi gestiscono.

Nell'era dei sensori e dell'intelligenza artificiale, dell'interconnessione dei sistemi informatici, in un mondo in continua trasformazione digitale dove i dati scorrono vertiginosamente attraverso i fili invisibili del ciberspazio DataConSec si impegna ogni giorno a governare tale complessità per portare valore ai propri clienti.

DataConSec è una società di consulenza specializzata nel fornire soluzioni personalizzate e servizi altamente



qualificati nel campo della protezione dei dati personali, della cybersecurity, della digital forensics, della continuità operativa e del whistleblowing a clienti in ambito mondo pubblico e privato appartenenti a molteplici settori.

Attraverso la nostra esperienza multidisciplinare aiutiamo i clienti a identificare, valutare e mitigare i rischi, offrendo un supporto costante per mantenere nel tempo la sicurezza e la conformità a leggi cogenti e standard di mercato.

La nostra squadra, composta da diverse professionalità con competenze legali, tecniche e organizzative, è continuamente impegnata a sviluppare modelli organizzativi e tecnologie a supporto della sicurezza del business e al governo delle informazioni.

# DATA CONSEC

DATA PROTECTION - CONSULTING - SECURITY

## MISSION

Attraverso la nostra esperienza multidisciplinare aiutiamo i clienti a identificare, valutare e mitigare i rischi, offrendo un supporto costante per mantenere nel tempo la sicurezza e la conformità a leggi cogenti e standard di mercato.

La nostra squadra, composta da diverse professionalità con competenze legali, tecniche e organizzative, è continuamente impegnata a sviluppare modelli organizzativi e tecnologie a supporto della sicurezza del business e al governo delle informazioni.

Siamo costantemente impegnati nella formazione, nell'educazione e nella consapevolezza, attraverso la collaborazione con università, istituzioni, associazioni di

categoria e aziende per costruire insieme una cultura della sicurezza in cui ogni individuo sia un alleato nel proteggere l'intera comunità digitale.

La conformità alle normative di settore e l'adozione delle migliori pratiche internazionali rappresentano i nostri fari: DataConSec sottopone da anni i processi di erogazione della consulenza e della formazione alle certificazioni ISO27001 e ISO 9001.

Con passione, innovazione e impegno per l'eccellenza, DataConSec lavora fianco a fianco ai propri clienti per affrontare le appassionati sfide del futuro.

### Team composto da:

- ▶ Avvocati specializzati in privacy e cybersecurity
- ▶ Responsabili della protezione dei dati (Data Protection Officer – DPO)
- ▶ Responsabili della conservazione digitale
- ▶ Consulenti di direzione aziendale
- ▶ Esperti di informatica forense e investigazioni digitali
- ▶ Esperti di sicurezza informatica
- ▶ Auditor certificati
- ▶ Project manager

# I NOSTRI SERVIZI



**Protezione  
dei dati**



**Consulenza  
di Direzione  
aziendale**



**Analisi dei  
rischi di cyber  
sicurezza**



**Cybersecurity**



**Direttiva NIS 2**  
Servizio di  
adeguamento alla  
Direttiva Europea



**Digital  
Forensics**



**Responsabile  
della conservazione  
digitale**



**Whistleblowing**  
Servizio di  
adeguamento  
alla normativa



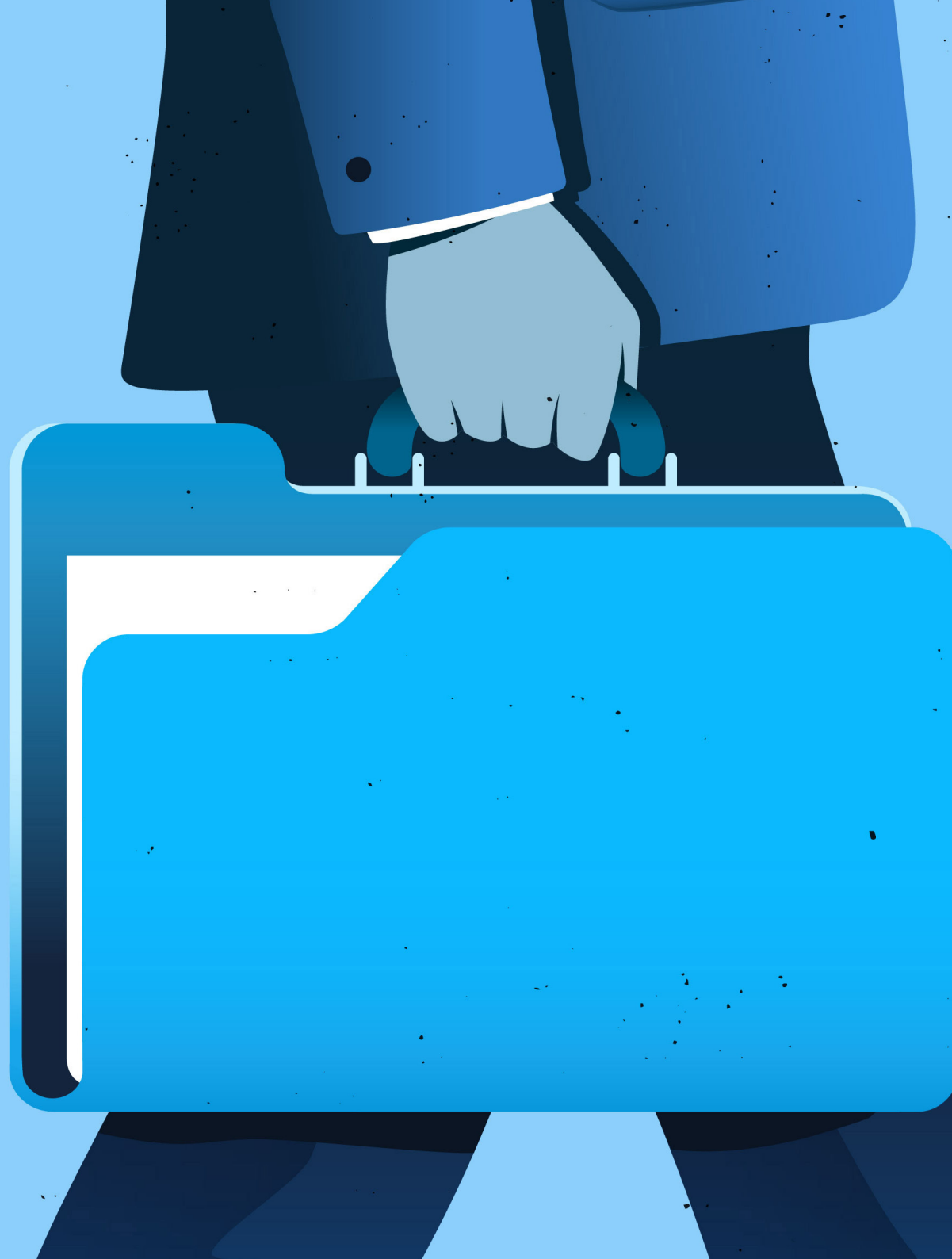
**ConceptLog**



**AEO**  
Operatore  
economico  
autorizzato



**FAD**  
Portale  
formazione



# PROTEZIONE DEI DATI

→ **Consulenza a 360° sulle regolamentazioni privacy italiane, europee e internazionali**

Nell'era digitale, in cui ogni passo lascia una traccia e ogni interazione genera dati, la tutela della privacy è diventata una delle principali sfide del nostro tempo e dunque al centro delle politiche legislative di tutti i Paesi più avanzati.

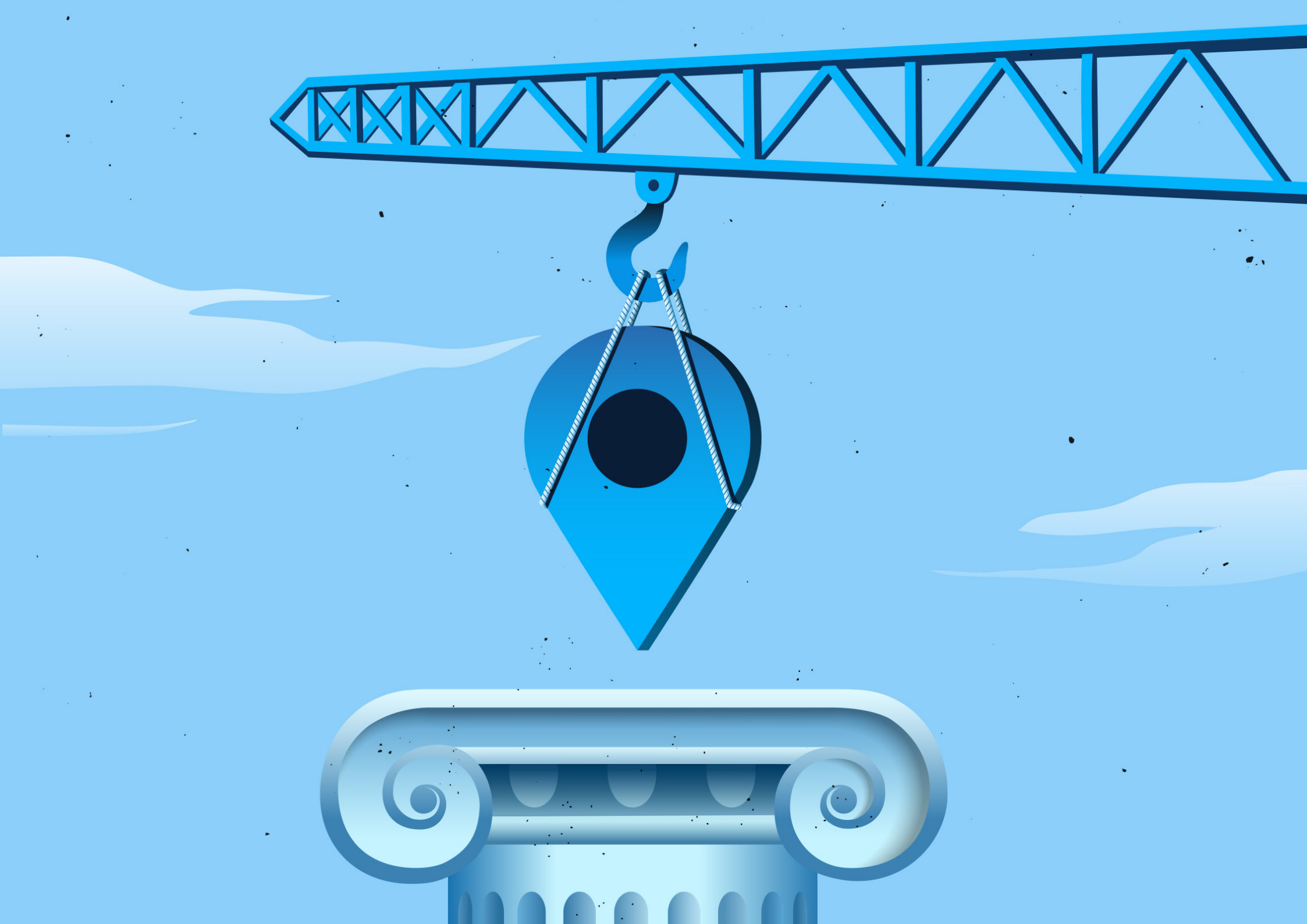
Il nostro servizio di consulenza in quest'ambito è una combinazione di **saggezza, competenza, esperienza maturata sul campo e approccio su misura** basato sul **rischio**.

Ci impegniamo a comprendere profondamente le esigenze e le specifiche dei clienti in ambito pubblico e privato operanti in molteplici settori, sviluppando una strategia di protezione dei dati personali che sia solida e al contempo agile da gestire. Siamo specializzati nella **risoluzione di problematiche** che prevedono il trattamento di dati personali in contesti tecnologicamente innovativi e complessi.

Creiamo e manteniamo aggiornati sistemi di gestione per la protezione dei dati personali e attraverso il nostro **approccio multidisciplinare** assumiamo formalmente il ruolo di Data Protection Officer in outsourcing.

## Servizi di consulenza in ambito privacy

- ▶ Data **governance** attraverso la stesura policy, procedure, linee guida e regolamenti interni
- ▶ Strategie di **accountability**
- ▶ Stesura di **informative** e contrattualistica ad hoc
- ▶ Privacy **by design** e **by default**
- ▶ Analisi del **rischio** privacy
- ▶ Supporto per l'adozione di **misure di sicurezza** tecniche e organizzative
- ▶ **Audit** di verifica sulle terze parti nominate Responsabili del trattamento
- ▶ Svolgimento di **valutazioni di impatto** privacy su nuove tecnologie
- ▶ Adempimenti di conformità per gli **amministratori di sistema** a log management
- ▶ Adeguamenti sistemi di **videosorveglianza**
- ▶ Attività di **due diligence**, valutazione della compliance in materia di dati personali a supporto delle attività di M&A
- ▶ **Pareri** tecnici e legali su questioni specifiche
- ▶ **Certificazioni** privacy
- ▶ Ruolo **DPO** in outsourcing
- ▶ **Formazione** multilivello personalizzata e in modalità e-learning



# CONSULENZA DI DIREZIONE AZIENDALE

- **Consulenza e progettazione sistemi di gestione e modelli organizzativi**
- **Strategie di gestione del rischio cyber**
- **Resilienza operativa digitale e continuità operativa**

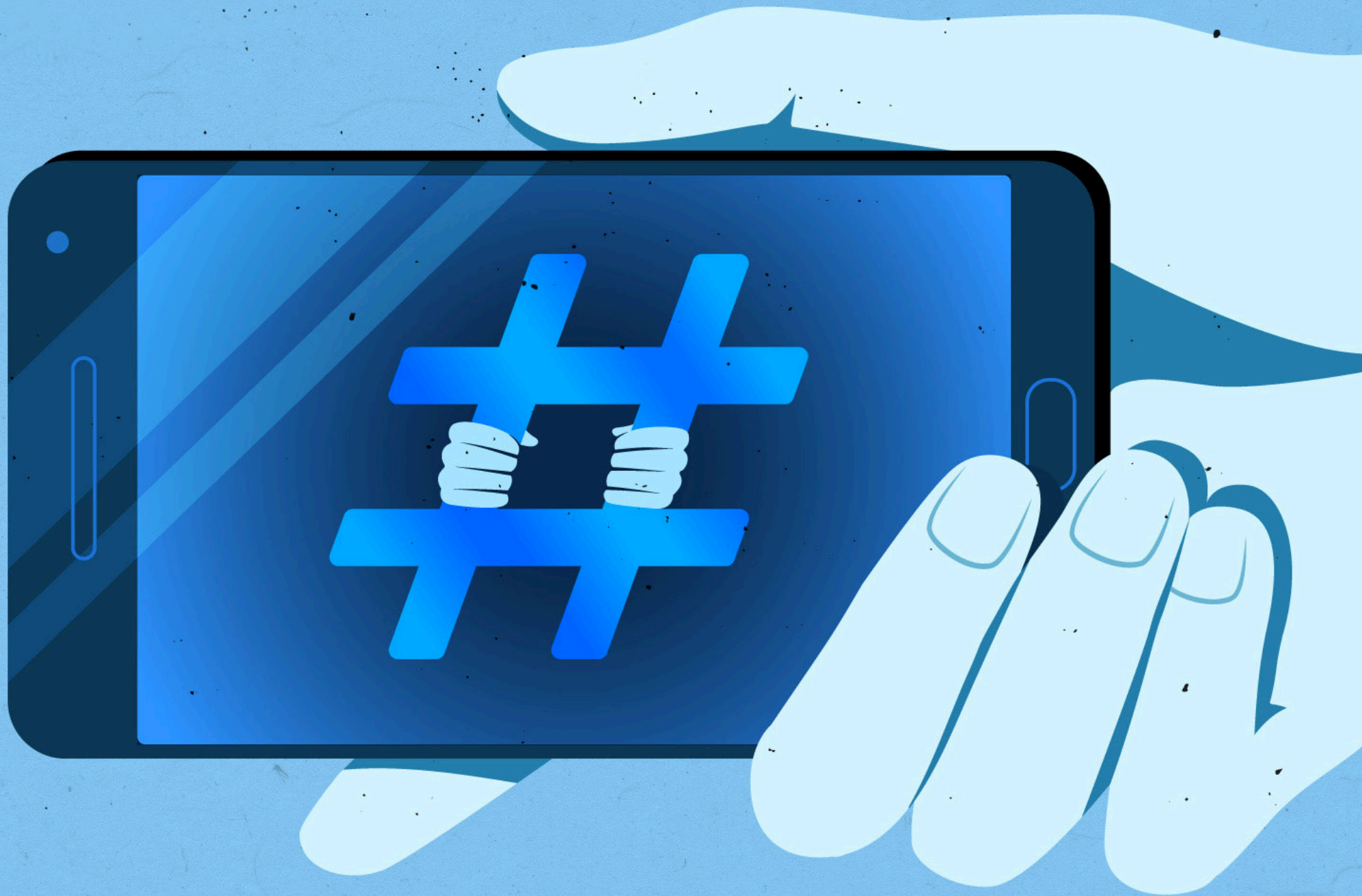
**DataConSec** può vantare all'interno del suo staff professionisti focalizzati nella governance della sicurezza delle informazioni.

L'ambito di specializzazione spazia alle attività di **Governance**, **Risk management** e **Compliance** svolte a beneficio di organizzazioni che operano in mercati regolamentati: bancario, assicurativo, cripto-attività, cloud computing, sanitario, farmaceutico, automotive, società quotate in borsa.

## Servizi di consulenza strategica

- ▶ Progettazione **sistemi di gestione** certificabili secondo norme internazionali
- ▶ Progettazione **modelli organizzativi 231** con focus sui reati informatici
- ▶ **Governance** attraverso la stesura policy, procedure, linee guida e regolamenti interni
- ▶ Strategie di accountability in ottica di **compliance** ICT
- ▶ Applicazione di metodologie di **analisi e gestione del rischio**
- ▶ Revisione dei **processi** e delle **procedure** per ottimizzare i flussi interni, migliorare l'efficienza e rafforzare la sicurezza
- ▶ Svolgimento di **Business Impact Assessment (BIA)** e stesura di Disaster Recovery Plan e Business Continuity Plan
- ▶ Supporto per l'adozione di misure tecniche e organizzative a supporto della **resilienza** operativa digitale
- ▶ **Audit** di conformità sulle terze parti
- ▶ Svolgimento di valutazione del rischio nell'applicazione di tecnologie di **intelligenza artificiale**
- ▶ Attività di **due diligence**, valutazione della compliance ICT a supporto delle attività di M&A
- ▶ **Pareri** tecnici e legali su questioni specifiche
- ▶ **Certificazioni** di prodotto e di processo con focus sulla qualità e la sicurezza delle nuove tecnologie
- ▶ Ruolo **OdV231** (con focus sui reati informatici) in outsourcing
- ▶ Ruolo **Responsabile** di sistemi di gestione in outsourcing
- ▶ **Formazione** multilivello personalizzata





# ANALISI DEI RISCHI DI CYBER SICUREZZA

→ **Protezione dei dati, del know-how  
e delle informazioni sensibili per il  
business**

Gli attacchi informatici sono sempre più frequenti, sofisticati e mirati.

Per qualsiasi organizzazione difendere le reti, i sistemi, gli applicativi, i dispositivi e quindi in ultima istanza i propri dati digitali è ormai essenziale per garantire la continuità operativa del business, **mantenere la fiducia del mercato** e tutelarsi da onerose sanzioni.

Il nostro approccio alla cybersecurity è frutto dell'**esperienza ventennale** maturata in contesti critici.

Progettiamo strategie e soluzioni personalizzate per difendersi da cyberattacchi, ransomware e data breach.

## Servizi di consulenza in ambito cybersecurity

- ▶ **Security governance** attraverso la stesura policy, procedure, linee guida e regolamenti interni.
- ▶ **Strategie** di cybersecurity e resilienza operativa digitale
- ▶ Analisi del **rischio cyber**
- ▶ Security **by design** e **by default**
- ▶ Attività di **Vulnerability Assessment and Management**
- ▶ Attività di **red teaming**
- ▶ Supporto per l'adozione di **misure di sicurezza** tecniche e organizzative in conformità a normative, best practices e standard internazionali
- ▶ **Supply chain** security attraverso audit di verifica sulle terze parti
- ▶ Analisi sicurezza **blockchain** e **smart contract**
- ▶ **Log management**
- ▶ **Gestione incidenti**
- ▶ **Due diligence**, valutazione della postura di sicurezza a supporto delle attività di M&A
- ▶ **Pareri** tecnici e legali su questioni specifiche
- ▶ **Certificazioni** in ambito cybersecurity
- ▶ Ruolo **CISO** in outsourcing
- ▶ Formazione multilivello personalizzata e in modalità e-learning

# CYBER SECURITY

- **Vulnerability assessment**
- **Log management**
- **Penetration testing**
- **Security assessment**

## Cyber Security

Supportiamo i Clienti nell'implementazione di controlli specifici sugli asset più esposti al rischio sicurezza, definendo i migliori strumenti di governo delle informazioni, che si traducono in maggiore produttività, crescita aziendale e contenimento dei costi.

## Cyber Strategy

Supportiamo l'azienda nell'analisi delle criticità relative alla cybersecurity sviluppando programmi di gestione del rischio coerenti con gli obiettivi strategici e il posizionamento dell'azienda stessa.

## Cyber Vigilance

Confrontiamo e analizziamo i dati sulle minacce legate alla cybersecurity aziendale per fornire ai responsabili aziendali del settore gli strumenti idonei ad individuare e gestire proattivamente le minacce informatiche, rispondendo tempestivamente agli incidenti informatici.

## Cyber Resilience

Attraverso protocolli e tecnologie proattive aiutiamo i Clienti ad adattarsi e rispondere alle minacce informatiche sia interne che esterne, per gestire al meglio la propria attività durante un Data breach o un cyber attacco.

## Vulnerability Assessment and Penetration Testing

Svolgiamo attività di Penetration Testing e Vulnerability Assessment sia manuali che automatizzati utilizzando "sonde" preparate ad hoc con diversi moduli a seconda delle esigenze del cliente.

Supporto successivo nella prevenzione di eventi dannosi quali la perdita e distruzione dei dati, interruzione o alterazione del servizio.



COMPUTER



SECURITY



ATTACK



HACKER



ALGORITHM



ACCESS



DIGITAL



CONFIDENCE

# DIRETTIVA NIS 2

→ **Adeguamento alla Direttiva Europea 2022/2555 (NIS 2: Network and Information Security 2)**

## 1. Direttiva NIS2: cosa è

La Direttiva NIS2, acronimo di “Network and Information Security 2”, è la nuova normativa europea (Direttiva 2022/2555) che sostituisce la precedente Direttiva NIS (2016/1148).

Questa normativa stabilisce un quadro comune per la sicurezza delle reti e dei sistemi informativi degli Stati Membri dell’UE, con l’obiettivo di uniformare le misure di sicurezza e rafforzare la resilienza informatica.

La Direttiva NIS2 introduce un approccio più coerente e collaborativo alla gestione della sicurezza informatica, affrontando le disparità tra i diversi Paesi dell’UE. Essa impone il coinvolgimento della direzione, requisiti

più rigorosi in termini di segnalazione degli incidenti, un approccio basato sul rischio e applicazione delle norme, per garantire un livello di sicurezza elevato e uniforme a livello europeo.

L’adeguamento alla Direttiva NIS2 comporta numerosi vantaggi, tra cui:

### ► **Riduzione dei rischi aziendali:**

Minimizza il rischio di incidenti di sicurezza informatica attraverso misure proattive di gestione delle informazioni.

### ► **Allineamento alle normative e alle best practice internazionali:**

Assicura che l’organizzazione sia in linea con il mercato e con le migliori pratiche globali in materia di sicurezza informatica.

### ► **Vantaggio competitivo:**

Rafforza la reputazione dell’azienda agli occhi di clienti e fornitori, dimostrando un impegno serio verso la sicurezza delle informazioni.

## 2. Perché adeguarsi alla Direttiva NIS2

Oltre a rispondere a un obbligo di legge per molte aziende, l’adeguamento volontario alla Direttiva NIS2 offre un’opportunità strategica per migliorare il sistema di gestione della sicurezza delle informazioni.

Implementare i requisiti minimi di sicurezza indicati dalla direttiva consente di identificare e risolvere criticità e di sviluppare un sistema più robusto.



Rendere la tua azienda conforme alla Direttiva NIS2 dimostra un livello adeguato di attenzione alla sicurezza informatica, cruciale anche per la sicurezza della supply chain. Inoltre, la conformità alla Direttiva NIS2 attesta ai clienti, fornitori e partner che l'azienda è affidabile e attenta alla protezione delle informazioni.

### 3. I nostri servizi per l'adeguamento alla Direttiva NIS2

► **GAP Analysis:**

Analisi delle lacune rispetto ai requisiti NIS2 per identificare aree di miglioramento.

► **Compliance NIS2:**

Supporto completo per l'allineamento dell'azienda alla direttiva.

► **Individuazione di standard/framework di sicurezza:**

Selezione degli standard e dei framework di sicurezza più adeguati per rispettare i requisiti normative (es. ISO 27001).

► **Internal Audit:**

Servizio di audit interno per verificare la conformità e migliorare i processi di sicurezza.

► **Audit ai fornitori (qualifica supply chain):**

Verifica della conformità dei fornitori alla direttiva per garantire la sicurezza della supply chain.

Questi servizi sono progettati per supportare le aziende in tutte le fasi di adeguamento alla Direttiva NIS2, garantendo la massima sicurezza e competitività sul mercato da parte di professionisti con competenze tecnico-giuridico-organizzative.

DATA CONSEC  
DATA PROTECTION - CONSULTING - SECURITY







# DIGITAL FORENSICS

- **Investigazioni digitali**
- **Consulenze tecniche**
- **Perizie informatiche**
- **Pareri tecnici e legali su questioni specifiche di informatica forense in ambito civile, penale, giuslavoristico e amministrativo**

In un'era digitale in continua evoluzione basata sull'interconnessione dei sistemi informatici, la digital forensics riveste un ruolo cruciale nell'affrontare frodi online e crimini informatici, preservando e analizzando prove provenienti da ambienti informatici complessi. Nella realtà odierna quasi tutti i casi trattati in un tribunale sia in ambito civile, penale, giuslavoristico, tributario che amministrativo coinvolgono in qualche misura dati digitali.

DataConSec vanta un'esperienza più che decennale in materia, sono stati gestiti centinaia di casi coprendo praticamente ogni ambito. Si sono svolte investigazioni digitali per conto di diverse Procure della Repubblica su computer, tablet, smartphone, dispositivi mobili e reti informatiche ricoprendo il ruolo di Consulente Tecnico

d'Ufficio (CTU) in procedimenti penali partecipando anche a delicate operazioni di acquisizione e sequestro a supporto dell'Autorità giudiziaria.

Operando come Consulente Tecnico di Parte (CTP) per conto di avvocati, studi professionali, organizzazioni pubbliche e private si sono svolte attività per frodi informatiche, furti di identità digitale, furti di informazioni riservate, violazione di policy e procedure aziendali, attacchi e incidenti informatici, data breach, spionaggio industriale, cybercrime, diffamazione on-line e stalking. DataConSec dispone di un **laboratorio forense certificato** secondo stringenti standard internazionali di sicurezza e qualità.

## Servizio di Digital Forensics

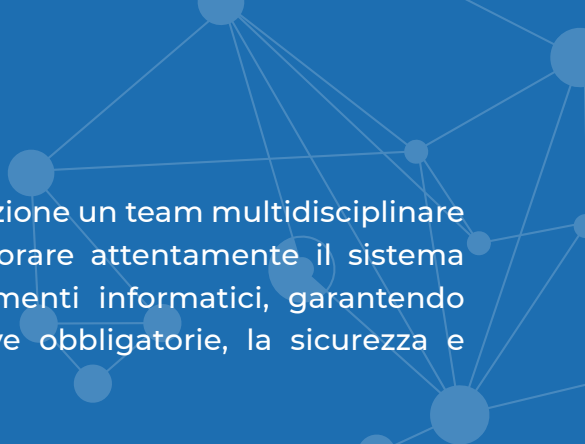
- ▶ Identificazione, acquisizione, preservazione, analisi, documentazione e presentazione di **prove digitali** contenute in PC, notebook, hard disk, chiavette USB, smartphone e tablet, server fisici e virtuali, database, siti web e social network, e-mail e posta elettronica, ecc.
- ▶ **Investigazioni digitali**
- ▶ **Consulenze tecniche**
- ▶ **Perizie informatiche**
- ▶ **Cristallizzazione** probatoria in caso di incidenti informatici, frodi, furti di proprietà intellettuale, brevetti, database commerciali
- ▶ **Pareri** tecnici e legali su questioni specifiche
- ▶ Ruoli **CTU, CTP**, periti per **polizze assicurative cyber**
- ▶ **Formazione** personalizzata di spionaggio, furto o danneggiamento dei dati, violazione delle policy aziendali.

# RESPONSABILE DELLA CONSERVAZIONE DIGITALE

La trasformazione digitale sta accelerando la smaterializzazione di documenti e atti di fondamentale importanza conferendo loro un valore, anche giuridico, per imprese e pubblica amministrazione.

Da qui l'importanza di dedicare la massima attenzione sin dalla creazione dei documenti, assicurandone l'archiviazione accurata, la disponibilità e la leggibilità a lungo termine.

Il Codice dell'Amministrazione Digitale (CAD) ha introdotto il ruolo chiave del Responsabile della Conservazione, un professionista esterno dotato di competenze giuridiche, informatiche e archivistiche di alto livello.



DataConSec mette a disposizione un team multidisciplinare in grado di creare e monitorare attentamente il sistema di conservazione dei documenti informatici, garantendo la conformità alle normative obbligatorie, la sicurezza e l'integrità a lungo termine.

## Servizio di Responsabile della Conservazione digitale di consulenza strategica

- Definizione delle **politiche** di conservazione e dei requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività svolte e delle caratteristiche del sistema di gestione documentale adottato
- Gestione del **processo** di conservazione al fine di garantire nel tempo la conformità alla normativa vigente
- **Monitoraggio** della corretta funzionalità del sistema di conservazione
- **Verifiche** periodiche dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi



- ▶ Predisposizione e aggiornamento del **manuale della conservazione** in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti
- ▶ Progettazione **sistemi di gestione** della conservazione digitale certificabili secondo norme internazionali
- ▶ Revisione dei **processi** e delle **procedure** per ottimizzare i flussi interni, migliorare l'efficienza e rafforzare la sicurezza
- ▶ Supporto per l'adozione di **misure di sicurezza** tecniche e organizzative a supporto della resilienza operativa digitale
- ▶ **Pareri** tecnici e legali su questioni specifiche
- ▶ Ruolo **Responsabile della conservazione** in outsourcing
- ▶ **Formazione** multilivello personalizzata

DATA CONSEC

DATA PROTECTION - CONSULTING - SECURITY



# WHISTLEBLOWING

*Il decreto legislativo n° 24/2023, recentemente pubblicato in Gazzetta Ufficiale, prevede che le aziende adottino specifici protocolli volti a agevolare la segnalazione di possibili illeciti.*

→ **Servizio di adeguamento alla normativa**

Il **whistleblowing** è un termine che viene utilizzato per indicare l'atto di segnalare irregolarità o comportamenti illegali all'interno di un'organizzazione.

Una persona che ha conoscenza di attività illecite o non etiche all'interno dell'azienda in cui lavora o con la quale ha a che fare, può decidere di segnalare attraverso opportuni canali tali comportamenti.

Le segnalazioni possono essere effettuate anche in modo anonimo e rappresentano una forma di tutela per la persona che le attua.

La legge mira a incentivare la collaborazione dei lavoratori per favorire l'emersione dei fenomeni corruttivi o altri reati all'interno di enti pubblici e privati.

L'introduzione di una disciplina ad hoc sul fenomeno del whistleblowing recepisce normative internazionali ed europee volte a rafforzare l'azione di prevenzione e contrasto di questi fenomeni, anche con la previsione di sistemi informatici che consentono ai lavoratori di segnalare in condizioni di sicurezza gli eventuali reati di cui vengono a conoscenza.

## **La norma si applicherà:**

- Dal **15 luglio 2023** a tutte le aziende private che hanno impiegato, nell'ultimo anno, una media di lavoratori superiore a **249**.
- dal **17 dicembre 2023** tutte le aziende private che hanno impiegato, nell'ultimo anno, una media di lavoratori superiore a **50**.

Sono previste sanzioni per le aziende inadempienti: l'ANAC potrà comminare **sanzioni** amministrative pecuniarie di importo variabile dai **10.000 euro** fino ad un massimo di **50.000 euro** in caso mancata implementazione dei canali di segnalazione.

Per la gestione degli adempimenti necessari alla conformità normativa DataConSec offre 3 tipologie di servizi:

**1.** Consulenza **tecnologica** in merito ai canali informatici sicuri:

- ▶ **Implementazione e configurazione software sia in modalità On-Premise che SaaS;**
- ▶ Personalizzazione a seconda del contesto del cliente;
- ▶ Manutenzione e supporto;
- ▶ Formazione.

**2.** Consulenza in merito alla **documentazione legale:**

- ▶ Supporto alla direzione e alle funzioni di controllo interno per la definizione di politiche di whistleblowing e procedure interne in linea con il contesto dell'organizzazione;
- ▶ Affiancamento alle funzioni interne coinvolte nei processi di whistleblowing per la definizione del contenuto dei moduli di raccolta delle segnalazioni;
- ▶ Supporto legale per gli adempimenti relativi alla protezione dei dati quali per esempio: informative, lettere di autorizzazione e nomine ad hoc, valutazioni di impatto, configurazioni privacy by design e by default;
- ▶ Formazione.

**3.** Servizio **“chiavi in mano”** che prevede sia la consulenza tecnologica che quella relativa alla documentazione legale.

DATA CONSEC  
DATA PROTECTION - CONSULTING - SECURITY



# CONCEPTLOG SERVIZI GESTITI DI LOG MANAGEMENT

→ Servizio di gestione Log dei profili privilegiati **“ConceptLog”**

La soluzione di Log Management **“ConceptLog”** ideata dalla **DataConSec**, prevede la raccolta dei log delle utenze amministrative o privilegiate definite all'interno dei sistemi e degli applicativi aziendali.

Il servizio è stato realizzato con l'obiettivo di consentire a tutte le organizzazioni aziendali, di rispondere in maniera semplice, facile e completa all'esigenza di gestire i Log dei profili privilegiati, come imposto dalle raccomandazioni della autorità Garante della Privacy di seguito riportata per completezza di informazione, e aderenti alla normativa vigente in materia di protezione dei dati personali (Regolamento europeo 2016/679 GDPR).

*Provvedimento “Amministratori di sistema”  
Misure e accorgimenti prescritti ai titolari dei  
trattamenti effettuati con strumenti elettronici  
relativamente alle attribuzioni delle funzioni di  
amministratore di sistema - 27 novembre 2008  
(G.U. n. 300 del 24 dicembre 2008 e modificato in  
base al provvedimento del 25 giugno 2009).*



Il sistema raccoglie un insieme di eventi specifici, conformi ai requisiti normativi e legati ai soli utenti privilegiati (Amministratori di Sistema), indicati dal Cliente ed oggetto del provvedimento.

Il servizio è gestito da DataConSec su infrastruttura cloud collocata in UE e dispone di strumenti di backup opportunamente cifrati al fine di garantire la riservatezza dei dati gestiti dal sistema.

L'archiviazione dei log di accesso degli Amministratori di Sistema (AdS), come da riferimento normativo, prevede un tempo di conservazione non inferiore ai sette mesi.

# OPERATORE ECONOMICO AUTORIZZATO

- **Esame procedure**
- **Pratiche gestionali e documentazione in azienda**
- **Analisi dei Rischi**
- **Piano Sicurezza**

L'Operatore Economico Autorizzato (OEA) è una certificazione riconosciuta a livello internazionale, concessa alle aziende coinvolte nelle attività di importazione e esportazione.

Questa designazione è volta a facilitare il commercio internazionale, fornendo benefici fiscali e semplificazioni procedurali agli operatori economici che dimostrano di aderire a rigorosi standard di sicurezza e conformità doganale.

Gli OEA godono di uno status privilegiato nelle operazioni doganali, con un accesso agevolato a regimi doganali semplificati e vantaggi che possono includere priorità nelle ispezioni, riduzione dei tempi di sdoganamento e minori controlli doganali.

DataConSec prevede l'attivazione di un team di progetto interdisciplinare per affiancare il cliente nell'ottenimento dell'**autorizzazione a "Status di AEO"**.

Fanno parte della squadra professionisti di comprovata esperienza e di complementare specializzazione in ambito doganale, di organizzazione aziendale e analisi dei rischi, sicurezza fisica, legale, fiscale ed informatica.

## Servizio di Operatore Economico Autorizzato

- ▶ Esame procedure, pratiche gestionali e **documentazione** presenti in azienda
- ▶ **Valutazione** analitica delle condizioni rilevanti per raggiungere lo Status AEO.
- ▶ Stima delle **aree di rischio** anche attraverso sopralluoghi on site
- ▶ Stesura del **piano di sicurezza**
- ▶ Stesura della documentazione di supporto al **sistema di gestione AEO**
- ▶ Assistenza durante la fase l'**audit dell'Agenzia delle dogane**
- ▶ **Formazione** multilivello

**Per maggiori approfondimenti, visita il sito internet dedicato:**

**[www.consulentiaeo.it](http://www.consulentiaeo.it)**





# PORTALE FORMAZIONE DATACONSEC ACADEMY

- **Corso sul regolamento GDPR**
- **Corso Sicurezza dei Dati Aziendali**
- **Corso Security Awareness**

I dati sono ormai diventati uno degli asset aziendali più preziosi. La formazione per la loro protezione fornisce le competenze necessarie per difendere queste risorse critiche da minacce interne ed esterne.

Investire nella formazione prepara il personale a **fronteggiare le sfide future nel campo della sicurezza**, mantenendo l'organizzazione al passo con i rischi derivanti dalle ultime tendenze e tecnologie.

La formazione inoltre assicura la comprensione e la conformità a regolamenti come il GDPR, riducendo il rischio di sanzioni legali, contrattuali e multe.

L'aumento delle **minacce cibernetiche** richiede un personale informato e consapevole.

La formazione fornisce le conoscenze per riconoscere, prevenire e affrontare attacchi cibernetici. Un team ben formato è fondamentale per creare una cultura di sicurezza all'interno dell'organizzazione. La formazione migliora la consapevolezza dei dipendenti, riducendo le vulnerabilità legate a comportamenti non sicuri.

La formazione inoltre prepara il personale a **gestire situazioni di emergenza** legate alla sicurezza dei dati.

Rispondere prontamente e in modo efficace a violazioni o incidenti contribuisce a minimizzare i danni.

Una solida sicurezza dei dati contribuisce a costruire la **fiducia dei clienti e dei partner commerciali**.

Dimostrare un impegno verso la protezione dei dati può migliorare la reputazione aziendale.

Gli incidenti di sicurezza possono comportare costi significativi, tra perdite finanziarie e danni alla **reputazione**.

Investire nella formazione in sicurezza dei dati può **prevenire incidenti costosi** e risparmiare risorse.

La formazione in sicurezza dei dati è un **investimento strategico** che contribuisce a garantire la resilienza aziendale e a proteggere il valore critico dei dati.

## I vantaggi dei nostri corsi

- ▶ Accessibilità H24
- ▶ Differenti device supportati
- ▶ Accountability
- ▶ Attivazione rapida
- ▶ Moduli Smart
- ▶ User Friendly
- ▶ Disponibilità in ITA/ENG

# DATAConSEC

DATA PROTECTION - CONSULTING - SECURITY

**DataConSec S.r.l.**  
**Business Security & IT Governance**

V.le Fratti, 56 - Parma (Italy)  
Tel. e Fax: +39 0521.771298  
e-mail: [info@dataconsec.com](mailto:info@dataconsec.com)  
[amministrazione@pec.dataconsec.com](mailto:amministrazione@pec.dataconsec.com)  
[www.dataconsec.com](http://www.dataconsec.com)

C.F. e P.IVA 02470920345

