

## Consulenza Sicurezza delle Informazioni ISO 27001 ISO/IEC 29151:2017

**La nuova guida** ISO/IEC 29151 "Information technology - Security techniques - Code of practice for personally identifiable information protection", messa a punto dai tre principali organismi internazionali di normazione, fornisce un prezioso punto di riferimento a governi e industria perché presenta un codice di buone pratiche per garantire la protezione dei dati personali.

### **Information technology — Security techniques — Code of practice for personally identifiable information protection.**

- 1 Scope
- 2 Normative references
- 3 Definitions and abbreviated terms
  - 3.1 Definitions
  - 3.2 Abbreviated terms
- 4 Overview
  - 4.1 Objective for the protection of PII
  - 4.2 Requirement for the protection of PII
  - 4.3 Controls
  - 4.4 Selecting controls
  - 4.5 Developing organization specific guidelines
  - 4.6 Life cycle considerations
  - 4.7 Structure of this Specification
- 5 Information security policies
  - 5.1 Management directions for information security
- 6 Organization of information security
  - 6.1 Internal organization
  - 6.2 Mobile devices and teleworking
- 7 Human resource security
  - 7.1 Prior to employment
  - 7.2 During employment
  - 7.3 Termination and change of employment
- 8 Asset management
  - 8.1 Responsibility for assets
  - 8.2 Information classification
  - 8.3 Media handling
- 9 Access control
  - 9.1 Business requirement of access control
  - 9.2 User access management
  - 9.3 User responsibilities
  - 9.4 System and application access control
- 10 Cryptography
  - 10.1 Cryptographic controls
- 11 Physical and environmental security
  - 11.1 Secure areas

- 11.2 Equipment
- 12 Operations security
  - 12.1 Operational procedures and responsibilities
  - 12.2 Protection from malware
  - 12.3 Backup
  - 12.4 Logging and monitoring
  - 12.5 Control of operational software
  - 12.6 Technical vulnerability management
  - 12.7 Information systems audit considerations
- 13 Communications security
  - 13.1 Network security management
  - 13.2 Information transfer
- 14 System acquisition, development and maintenance
  - 14.1 Security requirements of information systems
  - 14.2 Security in development and support processes
  - 14.3 Test data
- 15 Supplier relationships
  - 15.1 Information security in supplier relationships
  - 15.2 Supplier service delivery management
- 16 Information security incident management
  - 16.1 Management of information security incidents and improvements
- 17 Information security aspects of business continuity management
  - 17.1 Information security continuity
  - 17.2 Redundancies
- 18 Compliance
  - 18.1 Compliance with legal and contractual requirements
  - 18.2 Information security reviews
- 21 Annex A – Extended control set for PII protection (This annex forms an integral part of this Recommendation | International Standard.)
  - A.1 General
  - A.2 General policies for the use and protection of PII
  - A.3 Consent and choice
  - A.4 Purpose legitimacy and specification
  - A.5 Collection limitation
  - A.6 Data minimization
  - A.7 Use, retention and disclosure limitation
  - A.8 Accuracy and quality
  - A.9 Openness, transparency and notice
  - A.10 PII principal participation and access
  - A.11 Accountability
  - A.12 Information security
  - A.13 Privacy compliance
- Bibliography

## DA UNI Protezione dei dati personali. Linee guida ISO IEC ITU

### ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection.

La privacy ha assunto nuove dimensioni nel mondo iperconnesso. La crescente frequenza di violazioni di "high-profile data" ha spinto i Paesi di tutto il mondo a una riflessione su potenziali politiche e regolamenti.

Uno degli esempi più noti è il Regolamento generale sulla protezione dei dati della Commissione europea (Regolamento UE 2016/679) che entrerà in vigore il prossimo mese di maggio, con il quale si intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini (e residenti) dell'Unione Europea, sia all'interno che all'esterno dei confini UE. Le implicazioni saranno globali.

La necessità di proteggere i dati personali sta crescendo con urgenza con la trasformazione digitale di settori quali la sanità e i servizi finanziari. Sempre più organizzazioni stanno elaborando dati personali, in quantità sempre maggiori.

La nuova guida ISO/IEC 29151 | ITU-T X.1058 "Information technology - Security techniques - Code of practice for personally identifiable information protection", messa a punto dai tre principali organismi internazionali di normazione, fornisce un prezioso punto di riferimento a governi e industria perché presenta un codice di buone pratiche per garantire la protezione dei dati personali. Essa stabilisce gli obiettivi dei controlli sulla protezione dei dati, specifica quali controlli sono richiesti e fornisce le linee guida per la loro attuazione; mostra anche come la disposizione di tali controlli possa soddisfare i requisiti identificati dalla valutazione dei rischi e di impatto delle organizzazioni, rilevanti per la protezione dei dati personali.

La guida - sviluppata dall'ISO/IEC JTC 1/SC 27 "IT Security techniques" in collaborazione con ITU-T Study Group 17 - si basa sulla norma ISO/IEC 27001 (UNI CEI EN ISO/IEC 27001:2017 "Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti") con indicazioni aggiuntive specifiche per la protezione dei dati personali.



**Dasa-Rägister**

**IQ-1012-05**

Certificato NO.  
Certificate NO.

**2012-10-09**

Data di prima emissione  
First issue date

**2017-11-06**

Data di ultima emissione  
Last issue date

**2018-10-09**

Data di scadenza  
Expiry date

President & CE

Auditing Director

Dasa-Rägister S.p.A.  
Italy - 00071 Pomezia - Roma  
Via dei Castelli Romani, 22  
Tel. + 39 0691822002  
Fax: +39 069107120  
www.dasa-raegister.com  
Offices: Milano, Roma, Bari



ISO 9001:2015  
ISO 9001:2015  
ISO 9001:2015  
PRO N° 2458  
Membro degli Accordi di Mutuo Riconoscimento  
RA, IAF e ILAC  
Signatory of RA, IAF and ILAC  
Mutual Recognition Agreements

Dasa-Rägister S.p.A.

ENTE CERTIFICATORE CERTIFICA CHE IL SISTEMA DI GESTIONE PER LA QUALITÀ DI  
CERTIFICATION BODY CERTIFIES THAT THE QUALITY MANAGEMENT SYSTEM OF

**Consulenza Integrata S.r.l.**

Italia - 00195 Roma - Via Dardanelli, 15

È STATO VERIFICATO E TROVATO CONFORME AI REQUISITI DELLO STANDARD  
HAS BEEN ASSESSED AND FOUND IN COMPLIANCE WITH THE STANDARD REQUIREMENTS

**EN ISO 9001:2015**

Per le seguenti attività aventi come oggetto

Consulenza di direzione nei settori: Qualità, Ambiente, Salute e Sicurezza sui luoghi di lavoro, Medicina del Lavoro, Sistemi di Gestione Integrata, Sistemi di gestione secondo Dlgs 231/01, Sicurezza Alimentare, Privacy. Progettazione ed erogazione di corsi di formazione continua nei settori: Qualità, Ambiente, Salute e Sicurezza sui luoghi di lavoro, Medicina del Lavoro, Sistemi di Gestione Integrata, Sistemi di gestione secondo Dlgs 231/01, Sicurezza Alimentare, Privacy. Progettazione ed erogazione di piani formativi aziendali finanziati da fondi interprofessionali

For the following activities having as object

Managerial Consultancy in the following area: Quality, Environment, Health and Safety at Workplaces, Occupational Medicine, Integrated Management Systems, Management systems according to Dlgs 231/01, Food Safety, Privacy. Design and provision of continual training courses in the following area: Quality, Environment, Health and Safety at Workplaces, Occupational Medicine, Integrated Management Systems, Management systems according to Dlgs 231/01, Food Safety, Privacy. Design and provision of Business training courses financed by interprofessional funds

Settori - Sectors 35 - 37

Informazioni puntuali e aggiornate circa lo stato della presente Certificazione sono disponibili all'indirizzo [www.dasa-raegister.com](http://www.dasa-raegister.com).  
Punctual and updated information regarding this Certification is available at [www.dasa-raegister.com](http://www.dasa-raegister.com).

Riferirsi alla Documentazione del Sistema di Gestione Qualità dell'Organizzazione per i dettagli delle singole esclusioni ai requisiti della Norma ISO 9001:2015. La validità del presente Certificato è subordinata al rispetto delle prescrizioni del Regolamento di Certificazione Dasa-Rägister dei requisiti della Norma ISO 9001:2015, ad un programma di sorveglianza annuale e ad un riesame ogni tre anni.

Refer to the Documents of the Quality Management System of the Organisation for details regarding the exclusions to ISO 9001:2015 Standard requirements. The validity of this Certificate is subordinated by a full respect of that prescribed in Dasa-Rägister's Certification Regulation, of ISO 9001:2015 Standard requirements, to an annual surveillance programme and to a three yearly re-assessment.



**Consulenza Sicurezza delle Informazioni ISO 27001**

**Consulenza Privacy**

