



Privacy Manager

PROGRAMMA ANALITICO D'ESAME

Privacy Manager



Sommario

PRESUPPOSTI NORMATIVI	3
I sistemi di classificazione dei corsi	3
Il DigComp Framework	3
I livelli di padronanza	4
Livelli di apprendimento EQF	4
Rispondenza agli obiettivi dell'Agenda 2030	5
I CORSI IDCERT	6
Corsi per le competenze digitali	6
Corsi per altri tipi di competenze	6
Obiettivi del corso	7
Ottenimento della certificazione	7
Destinatari	8
IL PROGRAMMA ANALITICO	9
MODULO 1	9
Il ruolo del DPO/RPD	9
MODULO 2	11
Il regolamento privacy UE 2016/679 (GDPR)	11
MODULO 3	13
Il Codice dell'Amministrazione Digitale	13
MODULO 4	16
Trasferimento dati all'estero e privacy comparata	16

PRESUPPOSTI NORMATIVI

IDCERT per la produzione dei suoi corsi si ispira alle più recenti disposizioni europee nell'ambito della formazione con l'intento di fornire un'alta qualità formativa ed una corrispondente omogeneità di metodo tali da permettere a tutti coloro che seguono i suoi corsi e conseguono le sue certificazioni o attestazioni di poter spendere le competenze ed i titoli acquisiti con la certezza di spendibilità a livello europeo.

I sistemi di classificazione dei corsi

IDCERT in rispondenza ai più moderni e riconosciuti sistemi di valutazione delle competenze classifica i suoi corsi secondo i parametri espressi dal DigComp, dal quadro tecnico del sistema europeo di crediti per l'istruzione e la formazione professionale (ECVET). Riconosce, inoltre, come i valori della conoscenza e delle competenze possano avere un impatto positivo verso il raggiungimento degli obiettivi previsti dalla "Agenda 2030 per lo Sviluppo Sostenibile".

Il DigComp Framework

Il *DigComp*, nelle sue evoluzioni, rappresenta lo strumento attraverso il quale l'Europa intende fornire le linee guida per la formazione digitale per il cittadino, il lavoro e l'impresa.

Il *DigComp Framework* è stato sviluppato attraverso un ampio processo di analisi e confronto di quadri e modelli esistenti di competenze ICT, alfabetizzazione digitale, informazione e alfabetizzazione mediatica, per citarne solo alcuni.

Il *DigComp Framework* viene utilizzato per valutare, riconoscere e certificare i risultati di apprendimento delle competenze digitali.

Questo riconoscimento è importante sia per coloro che desiderano dimostrare già di avere competenze digitali sia per coloro che sono interessati a formarsi.

Per sintetizzare gli aspetti più salienti, il *DigComp* articola la sua strutturazione in 5 dimensioni:

Dimensione 1: Aree di competenze individuate come facenti parte delle competenze digitali.

Dimensione 2: Descrittori delle competenze e titoli pertinenti a ciascuna area.

Dimensione 3: Livelli di padronanza per ciascuna competenza.

Dimensione 4: Conoscenze, abilità e attitudini applicabili a ciascuna competenza.

Dimensione 5: Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Per maggiori approfondimenti sul *DigComp* riferirsi [qui](#).

Secondo questo schema IDCERT costruisce i syllabus, l'articolazione ed il sistema di valutazione dei suoi corsi.

I livelli di padronanza

Ciascun livello rappresenta un gradino in più nell'acquisizione da parte dei cittadini delle competenze in base alla sfida cognitiva, alla complessità delle attività che possono gestire e alla loro autonomia nello svolgimento dell'attività.

Sulla base di questo metodo IDCERT classifica i suoi corsi secondo il seguente *Proficiency level*:



Livelli di apprendimento EQF

L'EQF è un quadro basato sui risultati dell'apprendimento articolato su 8 livelli per tutti i tipi di qualificazioni, che funge da strumento di "traduzione" tra i diversi quadri nazionali delle qualificazioni.

I valori espressi da 1 ad 8 sono la combinazione coerente dei risultati di apprendimento, che possono essere valutati e validati autonomamente. I risultati dell'apprendimento sono suddivisi in *conoscenze*, *abilità* e *competenze* che corrispondono ad azioni attraverso le quali l'individuo dimostra di padroneggiare le competenze acquisite, in base a determinati criteri di performance e condizioni contestuali.

IDCERT classifica i suoi corsi indicandone il valore EQF.

Rispondenza agli obiettivi dell'Agenda 2030

“[Agenda 2030 per lo Sviluppo Sostenibile](#)” è un programma d'azione per le persone, il pianeta e la prosperità sottoscritto nel settembre 2015 dai governi dei 193 Paesi membri dell'ONU. Essa ingloba 17 Obiettivi per lo Sviluppo Sostenibile – *Sustainable Development Goals, SDGs* – in un grande programma d'azione per un totale di 169 *target* o traguardi. I Paesi si sono impegnati a raggiungere gli obiettivi previsti entro il 2030.

IDCERT sposa pienamente la strategia europea per lo sviluppo sostenibile dando il suo contributo nell'ambito della formazione ed in particolare per quella digitale.

I percorsi formativi di IDCERT propongono l'acquisizione di conoscenze e competenze che possono contribuire ai processi di empowerment delle persone e quindi al potenziamento delle loro capacità di resilienza che, nei nuovi scenari disegnati dall'*Agenda 2030 per lo sviluppo sostenibile*, trovano una loro piena collocazione. La partecipazione e l'appoggio di IDCERT a progetti ed iniziative valoriali in ambito sociale, ambientale ed economico aggiungono e rafforzano la sua aderenza a quegli obiettivi previsti dall'*Agenda* con un particolare focus su alcuni di essi.



I CORSI IDCERT

La certificazione IDCERT, così come le sue attestazioni, diventano titoli da aggiungere sul proprio CV, su LinkedIn, su Facebook ecc. a dimostrazione di essere in possesso di determinate competenze richieste dal mercato del lavoro.

Corsi per le competenze digitali

I corsi che rilasciano la **certificazione IDCERT** sono in linea con il *DigComp Framework*.

Il Framework DigComp viene utilizzato in tre domini principali in cui la competenza digitale è sempre più importante:

- **Formazione scolastica e formazione in generale.**
Il quadro normativo trova applicazione nell'istruzione a tutti i livelli, a partire dalla scuola, dove contribuisce ai risultati scolastici e al benessere dei bambini e i giovani.
- **Apprendimento permanente e inclusione.**
La competenza digitale è importante nella vita di tutti i giorni e la mancanza di tale competenza può esacerbare la condizione di chi è già in posizione di svantaggio o addirittura può contribuire all'esclusione sociale.
- **Occupazione e lavoro.**
La competenza digitale oggi è necessaria per un'ampia varietà di profili professionali e nel mondo del lavoro.

Corsi per altri tipi di competenze

Come già chiarito poc'anzi, IDCERT abbraccia in pieno la nuova filosofia europea sulla formazione che mira a fornire competenze classificabili e valutabili secondo criteri certi e condivisi. Alla luce di questo, IDCERT classifica tutti i suoi corsi non strettamente legati alle conoscenze digitali mutuando la medesima strutturazione prevista dal *DigComp*, rispettandone comunque i principi generali ove non fosse possibile una perfetta corrispondenza al framework a seguito della diversità delle materie trattate.

Obiettivi del corso

Il corso di **Privacy Manager** fornisce ai partecipanti gli strumenti pratici, attraverso modelli interattivi ed esercitazioni, per divenire responsabile e coordinare le attività di trattamento di dati personali. Il percorso formativo ha una durata di 200 ore.

Il manager della privacy è la figura che assiste il titolare nelle attività di coordinamento di tutti i soggetti che sono coinvolti nel trattamento di dati personali (responsabili, incaricati, amministratori di sistema, ecc.), garantendo il rispetto delle norme in materia di privacy e il mantenimento di un adeguato livello di protezione dei dati personali.

Il Privacy Manager, così come indicato nella Norma UNI 11697:2017, è un profilo pertinente a soggetti con un elevatissimo livello di conoscenze, abilità e competenze in uno specifico contesto organizzativo (sia esso un'area funzionale dell'organizzazione sia il settore di appartenenza della stessa) per garantire l'adozione di idonee misure organizzative nel trattamento di Dati Personali. In altre parole, è il Responsabile del Trattamento dei Dati Personali che coordina trasversalmente i soggetti coinvolti nell'organizzazione aziendale.

Su questi presupposti IDCERT può essere impiegata come standard nella definizione di programmi di certificazione .

Il percorso di certificazione è suddiviso in 2 moduli; per ciascuno di essi sono previsti:

- manuali PDF
- video lezioni
- esercitazioni
- esame finale.

Il percorso formativo può svolgersi interamente online sul sito *idcert.io* oppure offline presso le sedi dei *Competence Center* affiliati IDCERT.

La piattaforma web di proprietà è accessibile anche a persone con disabilità visiva e/o uditiva.

Ottenimento della certificazione

La certificazione si conclude con il superamento degli esami previsti alla fine di ogni modulo. L'esame si considera superato con il 75% di risposte corrette.

La certificazione IDCERT è l'unica certificazione italiana costruita interamente sul *DigComp Framework* e, quindi, l'unica in grado di attestare in maniera oggettiva le competenze digitali necessarie per operare correttamente come cittadini digitali

con i dispositivi (computer, smartphone e tablet), sia per lavoro che per uso personale, così come richiesto dal *DigComp*.

Destinatari

Il corso è indirizzato a tutte le figure professionali coinvolte in attività in ambito Privacy, ossia a coloro che vogliono qualificare le proprie competenze specifiche sulla protezione dei Dati Personali, mediante un valido attestato riconosciuto sia per il settore pubblico che privato; a coloro che vogliono maturare le competenze nell'ambito della protezione dei Dati Personali; a coloro che vogliono intraprendere il percorso per conseguire la qualifica di Data Protection Officer (DPO):

- Imprenditori
- Quadri aziendali
- Professionisti e consulenti d'impresa
- Studenti universitari e in materie giuridiche ed economiche
- Amministratori e dipendenti di Pubbliche Amministrazioni

IL PROGRAMMA ANALITICO

Esso è strutturato seguendo le impostazioni del *DigComp Framework*, rappresentando, per ogni **competenza** (colonna sinistra), i relativi **descrittori** (colonna centrale) e le **conoscenze, abilità e attitudini** applicabili ad ogni singola competenza (colonna destra).

In questo modo sono immediatamente identificabili le competenze previste, per ogni area di competenza, e le specifiche di raggiungimento di conoscenze, abilità e attitudini.

MODULO 1

Il ruolo del DPO/RPD

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. IL DATA PROTECTION OFFICER – RESPONSABILE PROTEZIONE DATI	1.1 Evoluzione della figura del Data Protection Officer (DPO)	1.1.1 Introduzione della figura
	1.2 Diritto del Consiglio d'Europa	1.2.1 La nomina del DPO all'interno della Convenzione n. 108 del 1981
	1.3 La Direttiva 95/46/CE	1.3.1 Il Considerando 49
	1.4 Regolamento CE 45/2001	1.4.1 Art. 24 del Regolamento CE 45/2001
	1.5 Il GDPR e il D.lgs 101/2018	1.5.1 Il D.Lgs 101/2018
2. NOMINA DEL DPO / RPD	2.1 L'obbligo di nomina di un DPO/RPD per le autorità pubbliche	2.1.1 Competenze specialistiche del DPO/RPD
	2.2 Compiti del DPO/RPD	2.2.1 Parere del DPO/RPD sulla valutazione d'impatto
	2.3 Linee guida dei Garanti Europei	2.3.1 Il principio di responsabilizzazione
	2.4 Concetto di Autorità Pubblica	2.4.1 Le raccomandazioni del WP29

3. LE ATTIVITA' DEL DPO/RPD	3.1 Attività principali	3.1.1 Considerando 97 del GDPR
	3.2 Il concetto di "Larga scala"	3.2.1 Modelli di trattamento su larga scala
	3.3 Monitoraggio regolare e sistematico	3.3.1 Modelli di monitoraggio regolare e sistematico
4. DESIGNAZIONE, COMPETENZE, MODALITA' CONTRATTUALI	4.1 Chi deve nominare il DPO/RPD	4.1.1 Criteri di nomina
	4.2 Competenze e capacità del DPO	4.2.1 Competenze richieste all'interno di organismi pubblici
	4.3 Contratto di servizi	4.3.1 Art. 37 paragrafo 7 del GDPR
5. POSIZIONE, AUTONOMIA E INDIPENDENZA DEL DPO/RPD	5.1 Necessità del coinvolgimento del DPO/RPD	5.1.1 Garanzie di coinvolgimento del DPO/RPD
	5.2 Necessità di risorse	5.2.1 Art. 38 paragrafo 2 del Regolamento UE 2016/679
	5.3 Autonomia e indipendenza del DPO/RPD	5.3.1 Le penalizzazioni 5.3.2 Clausole sull'indipendenza
6. CONFLITTI DI INTERESSE, RISCHI E RUOLI DEL DPO/RPD	6.1 Conflitto di interessi	6.1.1 Le buone prassi 6.1.2 Il Gruppo istituzionale UE sul conflitto d'interessi
	6.2 L'approccio basato sul rischio	6.2.1 Gli ordini di priorità
	6.3 Il ruolo del DPO/RPD nella tenuta del Registro delle attività di trattamento	6.3.1 La prassi consolidata in tema di tenuta registri

MODULO 2

Il regolamento privacy UE 2016/679 (GDPR)

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. DISPOSIZIONI GENERALI, PRINCIPI E DIRITTI DELL'INTERESSATO (artt. 1-23)	1.1 Capo I – Disposizioni generali	1.1.1 Ambito di applicazione materiale 1.1.2 Ambito di applicazione territoriale 1.1.3 Definizioni
	1.2 CAPO II – Principi	1.2.1 I principi applicati 1.2.2 La disciplina del consenso
	1.3 CAPO III – Diritti dell'interessato	1.3.1 L'informativa sui dati personali (Sezione 1-2) 1.3.2 Le modalità dell'informativa 1.3.2 "Rettifica e cancellazione" (Sezione 3) 1.3.3 Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche (Sezione 4)
2. TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO (artt. 24-43)	2.1 Obblighi generali	2.1.1 Privacy by design 2.1.2 La pseudonimizzazione 2.1.3 Privacy by default 2.1.4 Responsabile del Trattamento
	2.2 Sicurezza dei dati personali (sezione 2)	2.2.1 Misure tecniche e organizzative
	2.3 Valutazione d'impatto sulla protezione dei dati e consultazione	2.3.1 La valutazione d'impatto (art. 35 GDPR)
	2.4 Responsabile della protezione dei dati (sezi. 4)	2.4.1 DPO (Data Protection Officer)
	2.5 Codici di condotta e certificazione (Sezione 5)	2.5.1 I Codici di condotta 2.5.2 La certificazione

3. TRASFERIMENTO DATI VERSO PAESI TERZI E COMITATO EUROPEO PER LA PROTEZIONE DATI (artt. 44-76)	3.1 Trasferimento dei dati verso paesi terzi o organizzazioni internazionali.	3.1.1 Divieto di trasferimento 3.1.2 Ipotesi di trasferimento dati extra UE 3.1.3 Deroghe all'adeguatezza
	3.2 Il Comitato Europeo per la protezione dei dati	3.2.1 Art. 68 del GDPR 3.2.2 Linee guida del EDPB
4. SANZIONI, RESPONSABILITÀ E RIMEDI ARTT. 77 – 91	4.1 Le sanzioni	4.1.1 L'art. 83 del Regolamento UE 2016/679 4.1.2 L'art. 84 del GDPR 4.1.2 L'art. 84 del GDPR
	4.2 Responsabilità	4.2.1 L'art. 82 del GDPR 4.2.2 La responsabilità del DPO/RPD
	4.3 Rimedi	4.3.1 Tempi di decisione 4.3.2 Rappresentanza degli interessati

MODULO 3

Il Codice dell'Amministrazione Digitale

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. IL CODICE DELL'AMMINISTRAZIONE DIGITALE - STRUTTURA	1.1 Assetto del CAD	1.1.1 La suddivisione in articoli
	1.2 Ambito di applicazione	1.2.1 Aspetti organizzativi delle PA
	1.3 I diritti dei cittadini e delle imprese (sezione II)	1.3.1 I gestori dei pubblici servizi
	1.4 Organizzazione dell'e-Government nelle pubbliche amministrazioni	1.4.1 La governance 10
2. FORMAZIONE E SOTTOSCRIZIONE DEL DOCUMENTO INFORMATICO	2.1. Formazione del documento informatico	2.1.1 Differenza tra documento scritto e sottoscritto
	2.2 La sottoscrizione (sezione 2)	2.2.1 Firma elettronica e firma digitale organizzative
	2.3 Le copie di documenti informatici	2.3.1 L'art. 23 del CAD
	2.4 I certificatori di firma	2.4.1 I certificatori accreditati
3. LA GESTIONE E LA CONSERVAZIONE DEI DOCUMENTI (CAPO III)	3.1 Protocollo informatico	3.1.1 Il c.d. nucleo minimo
	3.2 Gestione informatizzata	3.2.1 Utilizzo di strumenti tecnologici
	3.3 Cooperazione applicativa	3.3.1 I sistemi di cooperazione
	3.4 Fascicolo informatico	3.4.1 Conservazione documento informatico
4. TRASMISSIONE INFORMATICA DEI DOCUMENTI (CAPO IV)	4.1 La posta elettronica	4.1.1 L'art. 45 del CAD 4.1.2 Distinzione tra consegna e disponibilità 4.1.3 L'art. 47 del CAD
	4.2 La posta elettronica certificata	4.2.1 La pec per le aziende 4.2.2 Rapporti tra pec e firma

		digitale
5. DATI DELLE PUBBLICHE AMMINISTRAZIONI, IDENTITÀ DIGITALI, ISTANZE E SERVIZI ON-LINE	5.1 I dati delle pubbliche amministrazioni	5.1.1 La fruizione del dato
	5.2 L' erogazione dei servizi on line	5.2.1 I livelli europei di interazione 5.2.2 La Legge n. 241 del 1990 26 5.2.3 I servizi on line delle PA: fruibilità 5.2.4 Pubblicazione di atti normativi e amministrativi 5.2.5 L'art. 65 del CAD
6. SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI (CAPO VI)	6.1 Lo sviluppo e l'acquisizione dei sistemi informatici da parte delle Pubbliche Amministrazioni	6.1.1 L'istituto del concorso di idee
	6.2 Il riuso	6.2.1 Le regole del riuso nel nuovo CAD
7. LE REGOLE TECNICHE (CAPO VII)	7.1 L'Autorità Informatica nella Pubblica Amministrazione	7.1.1 L'articolo 71 del CAD
8. IL SISTEMA PUBBLICO DI CONNETTIVITÀ – SPC	8.1 Il RUPA (Rete Unitaria della Pubblica Amministrazione)	8.1.1 Internet nelle PA
	8.2 SPC (Sistema Pubblico di Connettività)	8.2.1 L'articolo 76 del CAD
	8.3 Commissione di coordinamento	8.3.1 La governance del Sistema Pubblico di Connettività
	8.4 Rete internazionale delle pubbliche amministrazioni	8.4.1 Osmosi tra SPC e Rete Internazionale PA
9. DECRETO SEMPLIFICAZIONI E CODICE DELLA AMMINISTRAZIONE DIGITALE	9.1 Identità digitale, domicilio digitale e accesso ai servizi digitali	9.1.1 Il diritto di accesso
	9.2 SPID e CIE come unici strumenti di autenticazione	9.2.1 I livelli di sicurezza
	9.3 Diritto al domicilio digitale e relativi indici	9.3.1 Linee guida AgID
	9.4 Piattaforma per la notificazione digitale degli atti della Pubblica Amministrazione	9.4.1 Inclusione digitale delle persone con disabilità 9.4.2 Semplificazione anagrafica (ANPR)

		9.4.3 Pagamenti digitali: PagoPA e biglietti elettronici dei Comuni
	9.5 Governance della trasformazione digitale	9.5.1 Strategia digitale: coordinamento e attuazione 9.5.2 Codice di condotta tecnologica ed esperti 9.5.3 Disponibilità dei dati della PA 9.5.4 Piattaforma Digitale Nazionale Dati (PDND) 9.5.5 CED delle PA e migrazione in cloud
10. LA TRANSIZIONE DIGITALE DELLA PUBBLICA AMMINISTRAZIONE	10.1 La digitalizzazione nella Pubblica Amministrazione	10.1.1 La strategia di transizione digitale
	10.2 Il D.L. 22/2021 di riordino dei ministeri	10.2.1 Art. 8 D.L. 22 del 2021
	10.3 Comitato interministeriale per la transizione digitale	10.3.1 La segreteria tecnico-amministrativa del Comitato
	10.4 La Riforma della PA	10.4.1 Il programma di riforme
	10.5 La digitalizzazione della P.A. nel Piano Nazionale di Ripresa e Resilienza (PNRR)	10.5.1 La missione n. 1 del PNRR
	10.6 Indicazioni europee	10.6.1 Il Country Report 2020
	10.7 Strategia nazionale per le competenze digitali	10.7.1 I quattro assi di intervento
	10.8 Piano triennale per l'informatica nella p.a. e Strategia 2025	10.8.1 Le azioni di intervento
	10.8.1 Le azioni di intervento	
10.9 Le modifiche al Codice dell'amministrazione	10.9.1 Il nuovo CAD	

MODULO 4

Trasferimento dati all'estero e privacy comparata

Competenze	Descrittori delle competenze	Conoscenze, abilità e attitudini applicabili
1. LA CIRCOLAZIONE DEI DATI NELLE SOCIETÀ MULTINAZIONALI	1.1 Il DPO nelle multinazionali: la normativa di riferimento	1.1.1 L'art. 37 par. 2 del Regolamento UE 2016/679
	1.2 Gli obblighi del titolare	1.2.1 Linee Guida e Garanti Europei
	1.3 I contatti con le autorità	1.3.1 La gestione della Data Protection
	1.4 Il DPO nelle multinazionali: un adempimento necessario	1.4.1 L'accountability del Titolare del trattamento
	1.5 Multinazionali e GDPR	1.5.1 Estensione dell'ambito di applicazione del GDPR 1.5.2 Clausole di protezione dei dati 1.5.3 Deroghe
2. PRIVACY: PROFILI DI DIRITTO (COMPARATO)	2.1 Il concetto di privacy nel diritto americano	2.1.1 Pronunce giurisprudenziali statunitensi
	2.2 La nuova direttiva europea	2.2.1 Introduzione del GDPR 2.2.2 La Dichiarazione universale dei diritti dell'uomo 12 2.2.3 Le linee guida europee e la Convenzione n. 108 2.2.4 Trattato di Lisbona e Carta di Nizza 2.2.5 La Legge n. 675 del 1996 2.2.6 Il Decreto Legislativo n. 196 del 30 giugno 2003 2.2.7 Evoluzione normativa post 2012
	2.3 Un confronto tra le diverse realtà ordinamentali	2.3.1 La situazione nei paesi europei 2.3.2 Il caso Cambridge Analytica
	2.4 Riflessioni finali	2.4.1 Le principali innovazioni apportate dal Protocollo

3. SISTEMA DI GESTIONE E CONTROLLO DEI DATI	3.1 Sistema di gestione privacy e accountability	3.1.1 Il principio di accountability
	3.2 Sistema di gestione privacy: strutturare il modello organizzativo	3.2.1 I nuovi modelli di gestione
	3.3 La logica di un sistema di gestione privacy	3.3.1 Gli standard internazionali
	3.4 Sistema di gestione privacy: il metodo	3.4.1 Il ciclo di Deming
	3.5 Sistema di gestione privacy: il risk-based thinking	3.5.1 La valutazione del rischio
	3.6 Il sistema di gestione privacy: a cosa serve	3.6.1 Scopo del sistema di gestione privacy
	3.7 Struttura del sistema di gestione privacy	3.7.1 Il "contenitore" privacy
	3.8 Integrazione dei sistemi	3.8.1 I Sistemi di Gestione dell'azienda
	3.9 Intelleggibilità dei modelli organizzativi	3.9.1 Orizzonte internazionale dei requisiti
4. LE MISURE DI SICUREZZA TRA GDPR E ISO 27001	4.1 GDPR e sicurezza dei dati personali	4.3 ISO 27001:2017 e sicurezza
	4.2 Responsabilità	4.2.1 L'art. 82 del GDPR 4.2.2 La responsabilità del DPO/RPD
	4.3 ISO 27001:2017 e sicurezza delle informazioni	4.3.1 Il raggio di operatività
	4.4 GDPR E ISO 27001: una relazione imprescindibile?	4.4.1 Il Considerando 100 del GDPR
5. LA PRIVACY BY DESIGN IN UN CONTESTO DI COMPLIANCE CON LA ISO 9001	5.1 Privacy by design e ISO 9001: il quadro di riferimento	5.1.1 La UNI EN ISO 9001:2015 (Sistema gestione qualità)
	5.2 Privacy by design e ISO 9001: il giusto approccio	5.2.1 La compliant

6. L'AUDIT IN AMBITO PRIVACY	6.1 Approfondimenti tecnici negli audit privacy: a cosa servono	6.1.1 La UNI EN ISO 19011:2018
	6.2 La struttura di un'attività di audit di tipo tecnico	6.2.1 Le best practice
	6.3 Considerazioni	6.3.1 I piani di miglioramento

ChangeLog

versione 1.1

NOVITÀ

- Inserimento dell'indicazione del valore del corso secondo il quadro EQF basato sui risultati dell'apprendimento articolato su 8 livelli.
- Inserimento della rispondenza ai punti dell'Agenda per lo Sviluppo sostenibile.

AGGIORNAMENTI

- Adeguamento dei testi per una maggiore rispondenza a quanto previsto dal DigComp Framework.

DISCLAIMER

Il contenuto di questa dispensa (testi, immagini/foto/video, grafica, layout ecc.), ove non diversamente specificato, appartengono ad IDCERT S.r.l. e sono protetti dalla normativa sul diritto d'Autore e dalla normativa a tutela dei Marchi (L. 22 aprile 1941 n.633 e successive modifiche, R.D. n.929 del 21 giugno 1942 e successive modifiche) e sono coperti da copyright.

Fatti salvi gli utilizzi strettamente personali, non è consentito copiare, alterare, distribuire, pubblicare o utilizzare i contenuti della presente dispensa.

IDCERT fornisce questa dispensa a corredo del suo corso con la sola finalità di fornire il supporto per una sufficiente conoscenza degli argomenti trattati e per il conseguimento della certificazione / attestazione previste al termine del percorso di formazione.

I contenuti sono redatti con la massima cura e diligenza sottoponendo gli stessi ad accurato controllo.

IDCERT S.r.l., tuttavia, declina ogni responsabilità, diretta e indiretta, nei confronti degli utenti e in generale di terzi, per eventuali imprecisioni, errori, omissioni, danni (diretti, indiretti, conseguenti, punibili e sanzionabili) derivanti dai suddetti contenuti.

Tutti i marchi di terzi, loghi, nomi di prodotti, nomi commerciali, nomi di società eventualmente citati in questa dispensa sono marchi di proprietà dei rispettivi titolari o marchi registrati di altre società e sono stati utilizzati senza alcun fine di violazione dei diritti di Copyright vigenti.

L'indicazione dei predetti marchi e loghi è funzionale ad una mera finalità descrittiva ed esemplificativa degli argomenti del corso, nel rispetto di quanto disciplinato dal D.lgs. n.30 del 10 Febbraio 2005.

idcert[®] srl

Ufficio Italia - Europa

Via G. Pugnani 1
Andria - BT
T. 0883 885287



P.iva 08020870724
info@idcert.io

Ufficio California - Stati Uniti

2372 Morse Ave, Irvine,
CA 92614, United States

