AICA
ASSOCIAZIONE ITALIANA PER L'INFORMATICA
E IL CALCOLO AUTOMATICO



Protezione dati personali: GDPR, Privacy e Sicurezza

Syllabus 3.0

SCOPO

Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato. Il syllabus fornisce inoltre le basi per il test riguardante questo modulo.

COPYRIGHT © 2024 AICA

Tutti i diritti riservati. Questa pubblicazione non può essere riprodotta in alcuna forma se non dietro esplicito consenso di AICA.

PROTEZIONE DATI PERSONALI - GDPR, PRIVACY E SICUREZZA

Il seguente Syllabus riguarda è finalizzato alla conoscenza dei princìpi della protezione dei dati personali nella normativa europea

(Regolamento europeo sulla protezione dei dati - GDPR) e nella normativa nazionale.

OBIETTIVI DEL MODULO

Il modulo richiede che il Candidato conosca l'evoluzione del concetto di privacy, la normativa nazionale sulla privacy, i contenuti del Codice in materia di protezione dei dati personali (d.lgs.196/2003), del Regolamento europeo sulla protezione dei dati (GDPR), il ruolo dell'Autorità Garante e del Gruppo di lavoro "Articolo 29" (sostituito dal Comitato europeo per la protezione dei dati). Il Candidato deve comprendere le norme generali che regolano il trattamento dei dati personali e le particolarità di alcuni ambiti specifici di trattamento. Il Can-didato deve essere consapevole degli obblighi di sicurezza richiesti, della redazione della documentazione utile e necessaria a comprovare la conformità normativa, delle responsabilità e sanzioni previste dal Regolamento europeo sulla protezione dei dati (GDPR). Il Candidato deve conoscere le norme in materia di comunicazioni elettroniche non sollecitate e alcune particolari fattispecie di trattamenti illeciti.

Questa certificazione è indirizzata a responsabili della privacy e della protezione dei dati, Data Protection Of-ficer (DPO), responsabili dei sistemi informativi, tecnici informatici e consulenti informatici, dirigenti scolastici, insegnanti e formatori, responsabili di laboratori, funzionari e dipendenti della PA e degli Enti Locali, personale ap-partenente alle forze dell'ordine, giuristi, avvocati, magistrati, notai, commercialisti, ingegneri, dipendenti degli studi professionali.

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
1 Protezione dei dati personali e sicurezza	*1.1. Evoluzione della Privacy*	1.1.1	Conoscere l'origine e l'evoluzione del diritto alla privacy, dall'origine del concetto: "the right to privacy" alla Direttiva Europea 95/46/CE e al Regolamento UE 2016/679 (GDPR) e alla Carta di Nizza
		1.1.2	Comprendere il concetto di dato personale e di identificazione diretta o indiretta
		1.1.3	Saper valutare capacità identificativa, sensibilità e contesto del dato personale
		1.1.4	Comprendere gli ambiti di applicazione della norma nei trattamenti automatizzati e non automatizzati dei dati personali
		1.1.5	Comprendere le principali norme, linee guida ed interventi di portata internazionale che coinvolgono i dati personali
		1.1.6	Il futuro della privacy fra IoT, AI e dispositivi indossabili
	1.2 La Normativa europea e nazionale sulla Privacy	1.2.1	Conoscere la struttura del Regolamento UE 2016/679 (GDPR) e la normativa nazionale
		1.2.2	Conoscere il d.lgs. 101/2018 e le norme del Codice Privacy
		1.2.3	Conoscere le principali definizioni presenti nell'art. 4 del Regolamento UE 2016/679 - GDPR

Copyright © 2024 AICA

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.2.4	Comprendere i principi del Regolamento UE 2016/679 (GDPR): liceità, correttezza, trasparenza, limitazione delle finalita, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione
		1.2.5	Conoscere i diritti dei soggetti interessati (accesso, rettifica e cancellazione, limitazione di trattamento, obblighi di notifica in caso di rettifica o cancellazione dei dati, portabilità dei dati, diritto all'oblio, opposizione al trattamento)
		1.2.6	Comprendere il concetto di "profilazione" e conoscere i diritti di informazione ed opposizione al processi decisionali automatizzati
		1.2.7	Conoscere e saper identificare le principali tipologie di dati (dati personali e categoria particolare, dati genetici, dati biometrici, dati relativi alla salute, dati relativi a condanne penali e reati, dati che non richiedono l'identificazione)
		1.2.8	Comprendere il concetto di anonimizzazione e di pseudonimizzazione
		1.2.9	Identificare e riconoscere i ruoli, obblighi e responsabilità delle figure previste dal Regolamento UE 2016/679 - GDPR (Interessato, Titolare, Contitolare, Rappresentante del titolare, Responsabile del trattamento, Data Protection Officer, soggetto autorizzato) e dal d.lgs. 196/03Codice Privacy (Soggetto designato)
		1.2.10	Saper riconoscere i contenuti minimi e la struttura per redigere un'idonea informativa (definizione, funzione, contenuti obbligatori, modalità di rilascio e casi particolari) alla luce del Regolamento UE 2016/679 - GDPR
		1.2.11	Conoscere le informazioni ulteriori da dover fornire agli interessati secondo alcune norme specifiche come il Decreto trasparenza
		1.2.12	Comprendere il concetto di destinatario dei dati, comunicazione e diffusione
		1.2.13	Conoscere gli elementi essenziali per un consenso valido (informato, libero, specifico, inequivocabile, revocabile)
	1.3 L'Autorità di controllo e il Comitato europeo per la protezione dei dati	1.3.1	Conoscere compiti, funzioni e poteri delle autorità di controllo
		1.3.2	Conoscere il principio di one-stop-shop e le modalità di cooperazione fra autorità di controllo

Copyright © 2024 AICA

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.3.3	Conoscere la differenza fra reclamo e segnalazione
		1.3.4	Comprendere lo scopo del Comitato europeo per la protezione dei dati - EDPB
	1.4 *Specifici settori di trattamento*	1.4.1	Comprendere il concetto dell'interesse pubblico rilevante per le attività di trattamento svolte su dati personali
		1.4.2	Conoscere le peculiarità del trattamento dei dati personali in ambito sanitario
		1.4.3	Conoscere le peculiarità del trattamento dei dati personali nell'ambito della sicurezza pubblica
		1.4.4	Conoscere le peculiarità del trattamento dei dati personali nell'ambito della scuola e dell'istruzione
		1.4.5	Essere consapevoli delle responsabilità per quanto riguarda i minori e gli studenti
		1.4.6	Essere consapevoli delle normative specifiche e relative responsabilità riguardanti l'accesso ai servizi della società dell'informazione da parte dei minori da 14 a 18 anni
		1.4.7	Essere consapevoli delle normative specifiche e responsabilità riguardanti l'accesso ai servizi della società dell'informazione da parte dei minori di 14 anni
		1.4.8	Essere consapevoli del diritto alla protezione dei dati personali e dei diritti degli interessati nei settori in cui vigono obblighi di trasparenza amministrativa
	1.5 *La Sicurezza nelle operazioni di trattamento in base alle normative nazionali ed al Regolamento UE 2016/679 - GDPR*	1.5.1	Comprendere e saper applicare il concetto di analisi dei rischi riferito alle attività di trattamento dei dati personali
		1.5.2	Comprendere e saper applicare il concetto dello stato dell'arte nella gestione della sicurezza
		1.5.3	Comprendere e saper applicare il concetto di sicurezza del trattamento dei dati personali
		1.5.4	Comprendere i requisiti di riservatezza, integrita, disponibilita e resilienza dei sistemi e dei servizi a supporto del trattamento dati
		1.5.5	Conoscere la gestione di un incidente e l'approccio lesson learned
		1.5.6	Valutare le operazioni di salvataggio e ripristino operativo dei sistemi a seguito di incidenti

Copyright © 2024 AICA

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.5.7	Conoscere le misure di sicurezza tecniche e organizzative richiamate da specifici interventi dell'Autorità Garante
		1.5.8	Definire le procedure per testare l'efficacia delle misure di sicurezza
		1.5.9	Conoscere l'obbligo di istruzione dei soggetti che svolgono operazioni di trattamento sotto l'autorità del titolare e saperne valutare l'adeguatezza
		1.5.10	Conoscere gli obblighi specifici relativi agli amministratori di sistema
		1.5.11	Conoscere le misure di sicurezza relative alla gestione degli ambienti fisici
		1.5.12	Conoscere le misure di sicurezza relative alla gestione del fattore umano
	1.6 Obblighi generali del Titolare del trattamento	1.6.1	Identificare e riconoscere la documentazione che rendiconta le misure di sicurezza adottate
		1.6.2	Essere consapevole del concetto di Protezione dei dati fin dalla progettazione – Privacy by design
		1.6.3	Essere consapevole del concetto di Protezione dei dati per impostazione predefinita – Privacy by default
		1.6.4	Conoscere e comprendere i casi in cui è richiesto il registro dei trattamenti
		1.6.5	Conoscere gli obblighi riguardanti una violazione di dati personali – data breach: documentazione evento, notifica, comunicazione agli interessati
		1.6.6	Saper identificare i casi in cui è richiesta una valutazione d'impatto sulla protezione dei dati - Data Protection Impact Assessment (DPIA)
		1.6.7	Valutare i casi per la Consultazione preventiva e le relative modalità
		1.6.8	Conoscere la figura del Responsabile della Protezione dei dati o Data Protection Officer (DPO): designazione, posizione, requisiti e compiti
		1.6.9	Descrivere gli strumenti di autodisciplina a supporto della corretta applicazione della normativa (Codici di Condotta e Certificazioni)

Copyright © 2024 AICA

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.6.10	Conoscere e saper applicare le disposizioni sul trasferimento dei dati all'estero (extra-UE). Descrivere le condizioni di adeguatezza della Commissione, le norme vincolanti d'impresa e le clausole contrattuali tipo. Caso di studio specifico: la sentenza Schrems II e il trasferimento dei dati verso gli Stati Uniti
	1.7 Tipologie rilevanti di trattamento	1.7.1	Conoscere gli aspetti privacy nella videosorveglianza
		1.7.2	Comprendere le disposizioni privacy in materia di lavoro
		1.7.3	Essere consapevoli delle disposizioni in materia di posta elettronica del lavoratore
		1.7.4	Descrivere le peculiarità privacy dei siti web: peculiarità dell'informativa, acquisizione consensi e gestione cookie
		1.7.5	Comprendere le disposizioni riguardanti la privacy digitale: i log e loro conservazione, identificabilità e anonimato (anonymous surfing e remailing, fingerprinting)
		1.7.6	Definire la sicurezza come processo e conoscere le normative ISO riguardanti i Sistemi di Gestione per la Sicurezza delle Informazioni
		1.7.7	Conoscere differenze e similitudini tra web-app e mobile-app anche per la gestione dei dati personali
	1.8 Responsabilità del trattamento	1.8.1	Saper definire il concetto di rendicontazione degli adempimenti o accountability
		1.8.2	Conoscere l'applicazione delle sanzioni prevista dal Regolamento UE 2016/679 - GDPR.
		1.8.3	Comprendere le disposizioni sui danni cagionati per effetto del trattamento (responsabilità civile, diritto al risarcimento dei danni e inversione dell'onere della prova)
		1.8.4	Conoscere le Linee guida/opinion WP29 e la loro applicazione
	1.9 Reati che coinvolgono trattamenti di dati personali.	1.9.1	Comprendere gli aspetti legati al furto di credenziali (anche attraverso keylogger o malware) e il furto di identità
		1.9.2	Comprendere gli aspetti legati alla frode informatica e al phishing (fasi e reati configurabili)
		1.9.3	Comprendere gli aspetti legati alla commissione di reati tramite social network

Copyright © 2024 AICA

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.9.4	Comprendere gli aspetti legati alla diffamazione on line, via chat, al cyberbullismo e al cyberstalking
		1.9.5	Comprendere gli aspetti legati all'accesso abusivo a sistemi informatici e telematici, danneggiamento informatico e la violazione del domicilio informatico
		1.9.6	Comprendere gli aspetti legati al Revenge Porn, all'accesso e alla ridiffusione dei contenuti
2 Le comunicazioni non sollecitate	*2.1 Le comunicazioni elettroniche non sollecitate*	2.1.1	Comprendere il concetto di spam
		2.1.2	Conoscere il quadro normativo relativo alle comunicazione indesiderate, il concetto di opt-in e di opt-out
		2.1.3	Comprendere le modalità di formazione, acquisizione e controllo dei database "consensati"
		2.1.4	Identificare ruoli e responsabilità nelle supply chain riguardanti la gestione dei contatti di lead, prospect e clienti
		2.1.5	Comprendere l'eccezione del soft spam rispetto alle comunicazioni commerciali verso soggetti già clienti
		2.1.6	Conoscere gli elementi essenziali di cui tenere conto per l'invio di comunicazioni tramite newsletter
	2.2 Le Comunicazioni Telefoniche o con altri mezzi	2.2.1	Comprendere le disposizioni in materia di telemarketing
		2.2.2	Comprendere la differenza fra chiamate inbound e outbound

Copyright © 2024 AICA