



INFORMATICA GIURIDICA

**Protezione dati personali:
GDPR, privacy e sicurezza**

Syllabus 2.0

SCOPO

Il seguente Syllabus riguarda il modulo 1 *Protezione dati personali: GDPR, privacy e sicurezza* ed è finalizzato alla conoscenza dei principi della protezione dei dati personali nella normativa europea (Regolamento europeo sulla protezione dei dati - GDPR) e nella normativa nazionale.

COPYRIGHT © 2022 AICA

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

PROTEZIONE DATI PERSONALI - GDPR, PRIVACY E SICUREZZA

Il seguente Syllabus riguarda il modulo 2 Gestione Documentale e conservazione dei documenti digitali ed è finalizzato alla conoscenza dei principi 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 Candidato 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.

Questo modulo è indirizzato a responsabili della privacy e della protezione dei dati, Data Protection Officer (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 appartenente alle forze dell'ordine, giuristi, avvocati, magistrati, notai, commercialisti, ingegneri, dipendenti degli studi professionali.

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
1.1 Protezione dei dati personali e sicurezza	1.1.1 <i>Evoluzione della Privacy</i>	1.1.1.1	Conoscere l'origine e l'evoluzione del diritto alla privacy, l'origine del concetto: "the right to privacy" (dalla nascita, passando dalla Direttiva Europea 95/46/CE, arrivando sino al Regolamento UE 2016/679 - GDPR). Comprendere gli ambiti di applicazione della norma.
		1.1.1.2	Comprendere le principali linee guida e interventi legislativi internazionali, il ruolo dell'O.C.S.E. e del Consiglio d'Europa, la Convenzione di Strasburgo.
		1.1.1.3	Essere consapevole dell'evoluzione del diritto alla privacy nel proprio paese.
	1.1.2 <i>La Normativa europea e nazionale sulla Privacy</i>	1.1.2.1	Conoscere gli aspetti generali e la struttura del Regolamento UE 2016/679 - GDPR e la normativa nazionale.
		1.1.2.2	Comprendere i principi fondamentali del Codice della Privacy (finalità, necessità, liceità, correttezza, esattezza, proporzionalità, completezza, pertinenza e non eccedenza) e i principi riproposti dal Regolamento UE 2016/679 - GDPR (liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione).

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.1.2.3	Conoscere le principali definizioni presenti nel Regolamento UE 2016/679 – GDPR, ed i nuovi 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).
		1.1.2.4	Comprendere il concetto di “profilazione” e conoscere i diritti di opposizione ai processi decisionali automatizzati.
		1.1.2.5	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), e la pseudonimizzazione.
		1.1.2.6	Identificare e riconoscere i ruoli, obblighi e responsabilità delle figure previste dal Regolamento UE 2016/679 - GDPR (Interessato, Titolare, Co-titolare, Responsabile del trattamento, Data Protection Officer, Addetto al trattamento dei dati, Rappresentante del Titolare e del Responsabile), redigere e valutare le designazioni e le nomine.
		1.1.2.7	Comprendere differenze e similitudini tra l’informativa del Codice della Privacy del Paese e l’informativa prevista dal Regolamento UE 2016/679 - GDPR.
		1.1.2.8	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.
		1.1.2.9	Essere consapevoli dei significati attribuiti alle attività di comunicazione e diffusione dei dati.
		1.1.2.10	Comprendere l’importanza del consenso informato (funzione, contenuti e forma, il consenso nel trattamento di categorie particolari di dati, il rapporto tra consenso e informativa, condizioni applicabili al consenso dei minori, i casi di esclusione).
		1.1.2.11	Essere consapevole del diritto alla protezione dei dati personali e dei diritti degli interessati. Informazioni, comunicazioni e modalità trasparenti (ad es. Pubblica Amministrazione) per l’esercizio dei diritti dell’interessato.

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
	1.1.3 <i>L'Autorità di controllo e il Comitato europeo per la protezione dei dati</i>	1.1.3.1	Conoscere le funzioni dell'Autorità di controllo (compiti, competenze, poteri e controlli, segnalazioni, reclami, ricorsi e provvedimenti). One stop shop e cooperazione fra Data Protection Authority (DPA).
		1.1.3.2	Comprendere lo scopo del Comitato europeo per la protezione dei dati.
	1.1.4 <i>Specifici settori di trattamento</i>	1.1.4.1	Comprendere le attività di trattamento eseguite dai soggetti pubblici e le finalità di rilevante interesse pubblico; il trattamento in anagrafi ed elettorale; scopi storici e scientifici. Linee guida Nazionali e/o regolamenti tecnici specifici per la Pubblica Amministrazione.
		1.1.4.2	Conoscere il trattamento in ambito sanitario.
		1.1.4.3	Conoscere il trattamento in ambito giudiziario e nelle forze di polizia e di sicurezza.
		1.1.4.4	Essere consapevoli degli aspetti del trattamento delle informazioni nella scuola e istruzione; essere consapevoli delle implicazioni e delle responsabilità per quanto riguarda i minori e gli studenti.
	1.1.5 <i>La Sicurezza nelle operazioni di trattamento in base alle normative nazionali ed al Regolamento UE 2016/679 - GDPR</i>	1.1.5.1	Comprendere lo stato dell'arte riguardo agli obblighi di sicurezza previsti dal Regolamento UE 2016/679 - GDPR, anche in virtù dello sviluppo tecnologico, con l'obiettivo di minimizzare i rischi a carico dei dati. Conoscere Misure minime ed idonee in riferimento alla normativa nazionale ed europea.
		1.1.5.2	Essere consapevoli della necessità di compiere un'analisi dei rischi concernenti le operazioni di trattamento e valutare le misure adeguate di sicurezza per i trattamenti.
		1.1.5.3	Comprendere le tecniche di valutazione dei rischi.
		1.1.5.4	Descrivere e comprendere i concetti di anonimizzazione e di pseudonimizzazione.
		1.1.5.5	Comprendere i requisiti di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi a supporto del trattamento dati.
		1.1.5.6	Valutare le operazioni di salvataggio e di ripristino dell'accesso ai sistemi a seguito di incidenti fisici o tecnici.
		1.1.5.7	Conoscere i Provvedimenti generali, specifici e di semplificazione e le istruzioni dell'Autorità Garante alla luce del Regolamento UE 2016/679 - GDPR

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.1.5.8	Definire le procedure per testare l'efficacia delle misure tecniche.
		1.1.5.9	Essere consapevole dell'obbligo di istruzione delle figure che trattano i dati sotto l'autorità del Titolare o del Responsabile. Conoscere responsabilità e compiti degli Amministratori di sistema.
		1.1.5.10	Definire le Misure di sicurezza per i trattamenti senza l'ausilio di strumenti elettronici.
	1.1.6 <i>Obblighi generali del Titolare del trattamento</i>	1.1.6.1	Identificare e riconoscere la documentazione che comprova le misure di sicurezza adottate (dal DPS alle nomine sino al registro dei trattamenti e alla valutazione d'impatto). Identificarne gli scopi e le tempistiche per l'adeguamento.
		1.1.6.2	Essere consapevole dei concetti di Protezione dei dati fin dalla progettazione - Privacy by design.
		1.1.6.3	Comprendere il concetto di Protezione per impostazione predefinita - Privacy by default.
		1.1.6.4	Conoscere e comprendere i casi in cui è richiesto il registro delle operazioni di trattamento.
		1.1.6.5	Descrivere i contenuti e conoscere le tempistiche per la notifica di una violazione (c.d. data breach) all'autorità di controllo e comunicazione della violazione all'interessato.
		1.1.6.6	Saper identificare i casi in cui è richiesta una valutazione d'impatto sulla protezione dei dati (PIA) - Data Protection Impact Assessment (DPIA).
		1.1.6.7	Valutare i casi per la Consultazione preventiva e le relative modalità.
		1.1.6.8	Conoscere la figura del Responsabile della Protezione dei dati o Data Protection Officer - DPO (designazione, posizione, requisiti e compiti).
		1.1.6.9	Descrivere gli strumenti di autodisciplina a supporto della corretta applicazione della normativa (Codici di Condotta e Certificazioni).
		1.1.6.10	Conoscere e saper applicare le disposizioni sul trasferimento dei dati all'estero (extra- UE). Descrivere le condizioni di adeguatezza della Commissione e le norme vincolanti d'impresa. Caso di studio specifico: dal Safe Harbour al Privacy shield.
	1.1.7 <i>Tipologie rilevanti di trattamento</i>	1.1.7.1	Conoscere gli aspetti della privacy nel mondo del lavoro.

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
		1.1.7.2	Comprendere le disposizioni sulla videosorveglianza e GPS.
		1.1.7.3	Essere consapevoli delle disposizioni sulla privacy e posta elettronica.
		1.1.7.4	Descrivere la privacy su Internet: modalità di informative e consensi su web e in via telematica (normativa sui cookie).
		1.1.7.5	Comprendere le disposizioni riguardanti la privacy digitale: i log e loro conservazione, identificabilità e anonimato (anonymous surfing e remailing, cookies).
		1.1.7.6	Definire la sicurezza come processo e conoscere le normative internazionali ISO riguardanti i Sistemi di Gestione per tutela e sicurezza dell'informazione.
		1.1.7.7	Conoscere le differenze e le similitudini tra web-app e mobile-app riguardo all'informativa e consenso per il trattamento dei dati.
	1.1.8 <i>Tipologie rilevanti di trattamento</i>	1.1.8.1	Saper definire la Responsabilità per la rendicontazione (Accountability).
		1.1.8.2	Conoscere le sanzioni previste dal Regolamento UE 2016/679 - GDPR.
		1.1.8.3	Comprendere le disposizioni sui danni cagionati per effetto del trattamento (responsabilità civile, diritto al risarcimento e inversione dell'onere della prova).
		1.1.8.4	Saper valutare i casi per l'effettuazione dei ricorsi da parte degli interessati
		1.1.8.5	Conoscere le Linee Guida/opinion del WP29; Il diritto privacy nazionale e i rapporti con il Regolamento UE 2016/679 - GDPR.
	1.1.9 <i>Privacy e particolari casi di trattamento illecito</i>	1.1.9.1	Comprendere gli aspetti legati al furto di credenziali (anche attraverso keylogger e virus) e il furto d'identità.
		1.1.9.2	Comprendere gli aspetti legati alla frode informatica e al phishing (le sue fasi e i reati).
		1.1.9.3	Essere consapevoli degli aspetti di tutela della privacy nei social network.
		1.1.9.4	Conoscere la privacy collegata alla diffamazione on line, chat, cyberbullismo, cyber-stalking.
		1.1.9.5	Comprendere gli aspetti legati all'accesso abusivo a sistemi informatici e telematici, danneggiamento informatico e la violazione del domicilio informatico.

SEZIONI	ELEMENTI DI CONOSCENZA	RIF	ARGOMENTO
1.2 Le comunicazioni non sollecitate	1.2.1 <i>Le comunicazioni elettroniche nonv sollecitate</i>	1.2.1.1	Saper definire il concetto di spamming.
		1.2.1.2	Conoscere il quadro normativo sulle comunicazioni indesiderate e opt-in, optout.
		1.2.1.3	Essere consapevole degli aspetti per la prevenzione.
		1.2.1.4	Identificare o riconoscere le responsabilità e le sanzioni.
		1.2.1.5	Comprendere le disposizioni in materia di telemarketing.
	1.2.2 <i>Le Comunicazioni Telefoniche o con altri mezzi</i>	1.2.2.1	Conoscere la riservatezza e il quadro normativo sulle comunicazioni indesiderate.