PERCORSO BASE GDPR AGGIORNAMENTO

(Art. 29 GDPR - Regolamento UE 2016/679)

GDPR ZUCCHETTI **E-LEARNING**

ZUCCHETTI

DESTINATARI

Il corso si rivolge a tutti coloro che necessitano di una formazione di aggiornamento al fine di consolidare la formazione ottenuta con la frequenza del "Percorso base GDPR".

OBIETTIVO DEL CORSO

L'obiettivo è di consolidare la consapevolezza già creata nei dipendenti col corso Base, al fine non solo di sensibilizzarli sui temi relativi alla protezione dei dati personali, ma anche di avere del personale competente in materia.

"Solo creando consapevolezza si crea terreno fertile affinché la formazione attecchisca e le istruzioni (doverosamente fornite) vengano metabolizzate e seguite al fine di un costante e corretto trattamento dei dati garantendo l'accountability" (tratto dal corso in oggetto)

ATTESTAZIONI DI FREQUENZA

Ogni partecipante riceverà, previo sostenimento di un test superato con esisto positivo, un attestato di frequenza. L'attestato sarà rilasciato dalla piattaforma a completamento del corso e potrà essere scaricato e/o inviato tramite indirizzo e-mail.

DURATA COMPLESSIVA DEL CORSO

30 minuti

RIFERIMENTI NORMATIVI

Regolamento Europeo (UE) 2016/679

Provvedimenti dell'Autorità Garante per la protezione dei dati personali italiana

METODOLOGIA DEL CORSO

Corso online in modalità E-Learning asincrona

IDENTIFICATIVO DEL CORSO

GDPR_AGGIORNAMENTO_1.0

CONTENUTI DEL CORSO

MODULO	CONTENUTI	VERSIONE DEL MODULO
Consapevolezza nella gestione dei dati personali	La consapevolezza ("in pratica") nel trattamento dei dati personali inizia con la consapevolezza nella gestione dei propri dati personali e per la precisione nel comprendere perché/ a quale scopo sto dando i miei dati, a "chi" e questi entro quali limiti può trattarli (dati trattati nel rapporto di lavoro).	v.1.0
Doppio ruolo privacy del dipendente	La consapevolezza passa anche dalla comprensione di quale sia il proprio ruolo (privacy) nell'ambito dell'Azienda per cui si lavora. La necessità di conoscere i vari ruoli privacy è fondamentale perché aiuta a comprendere quale ruolo si ricopre in quale contesto e pertanto quali sono le regole che devono essere seguite. Il dipendente, nell'ottica del rapporto	v.1.0

	contrattuale di lavoro (quindi nel rapporto datore di lavoro-dipendente) ricopre il ruolo di “interessato” nel momento in cui fornisce i propri dati al fine della definizione del contratto di lavoro e della propria mansione lavorativa; al contempo e nel momento in cui, in forza di quel contratto di lavoro, svolge la propria attività professionale per la quale è richiesto anche il trattamento dei dati personali, ricopre anche il ruolo di “autorizzato” del trattamento.	
Documentazione che deve essere ricevuta	Per poter ricoprire correttamente ed efficacemente il doppio ruolo, il dipendente deve ricevere la documentazione necessaria: da un lato, in qualità di interessato del trattamento, affinchè sia a conoscenza di tutte le informazioni relative al trattamento dei propri dati personali (informativa) ad opera del datore di lavoro (titolare del trattamento) e dall’altro, in qualità di autorizzato, affinchè sappia quali sono le regole interne, le prassi e le linee guida della propria Azienda nell’utilizzo degli strumenti aziendali e nel trattamento dei dati personali di soggetti terzi (es. clienti, fornitori o dipendenti in base alla propria mansione).	v.1.0
Violazioni dei dati e errore umano	Una volta che il dipendente ha in mano i documenti necessari per un corretto trattamento di dati, necessita anche di una formazione mirata affinchè sia soggetto attivo e in grado di comprendere quanto è cruciale il ruolo che ricopre nella tutela della protezione dei dati personali trattati. Il dipendente deve sapere come muoversi per non violare dati e come evitare di essere fonte di potenziali data breach (violazione di dati personali). Quindi partendo dalle informazioni pratiche su cosa sia un data breach e quali possano essere le possibili fonti di violazione, affinchè si arrivi ad “agire” la protezione dei dati personali, prima è necessario che il dipendente prenda atto del fatto che la gran parte delle violazioni ha base interna (non muta che la fonte sia di base involontaria: dipendenti superficiali/poco formati o volontaria: dipendenti infedeli) e poi deve avere linee su come riconoscerli e nel caso gestirli.	v.1.0

Risposte: misure (tecniche e organizzative)	Una volta conosciute le fonti di rischio è necessario che il dipendente conosca l'esistenza di misure di sicurezza da attuare a protezione (per eliminare o ridurre il rischio). La formazione risponde a questo mediante: 1) spiegazione e identificazione delle diverse tipologie di misure di sicurezza; 2) esemplificazione di alcune regole interne (o procedure, a tutela della protezione dei dati) che il datore deve identificare e specificare negli appositi documenti da fornire al lavoratore e quest'ultimo poi deve conoscere; 3) identificazione dei documenti giusti per le informazioni giuste (ossia ad es. dove trovare le regole di utilizzo degli strumenti aziendali nel rispetto della normativa privacy; piuttosto che sapere quali sono le banche dati a cui ha accesso in base alla propria funzione ...); 4) trattazione di un caso, potenziale fonte di data breach.	v.1.0
Esercizio dei diritti e conclusioni	Con il caso del punto precedente si introduce anche il discorso relativa all'esercizio dei diritti degli interessati (e all'obbligo di risposta). Argomento di fondamentale importanza per la compliance aziendale e che dovrebbe essere oggetto di formazione specifica oltre a dover essere oggetto di specifica procedura da parte del datore di lavoro. In conclusione, poiché la protezione dei dati è una questione aziendale, ossia deve coinvolgere l'azienda in toto (ognuno col proprio ruolo e apporto) e deve essere gestita continuamente, ogni giorno, la formazione si chiude con una sintesi di "cosa fare" e "cosa non fare" in azienda nel rispetto della normativa privacy e quali sono gli elementi fondamentali affinchè la gestione dei dati personali sia fatta in maniera corretta ed efficace.	v.1.0

★ REQUISITI DI SISTEMA NECESSARI PER FRUIRE DEL CORSO

Connessione Internet	Stabile e velocità minima 1Mbit
Sistema operativo	Windows (XP o superiore), Mac OS X (10.6 o superiore)
Browser	Google Chrome (raccomandato), Edge, Mozilla Firefox, Safari
Impostazioni Browser	JavaScript abilitato Cookies abilitati Localstorage abilitato Livello di privacy e protezione consigliati: medio, medio alta
Plugin/Funzionalità browser richieste	Supporto HTML5

★ MODALITÀ DI ISCRIZIONE

L'utente potrà accedere alla piattaforma inserendo le proprie credenziali di accesso (mail e password o username e password).

★ MODALITÀ DI TRACCIAMENTO DELLE ATTIVITÀ

La piattaforma è dotata del sistema di gestione LMS, in grado di monitorare e certificare:

- Lo svolgimento e il completamento delle attività didattiche di ciascun utente
- La tracciabilità di ogni attività svolta durante il collegamento al sistema e la durata
- La presenza attiva dell'utente
- La tracciabilità delle singole unità didattiche strutturate in Learning Object (oggetto didattico), che contiene una serie di strumenti, quali il testo della lezione, l'audio che spiega gli argomenti, documenti di approfondimento, brevi filmati di esempio ed animazioni
- La modalità e il superamento delle valutazioni di apprendimento

La tracciabilità dei dati della piattaforma, degli accessi dell'utente e degli attestati viene conservata dalla piattaforma nei termini previsti dalla legge.

★ MODALITÀ DI VERIFICA DELL'APPRENDIMENTO

La verifica dell'apprendimento viene svolta tramite un test finale volto al consolidamento delle conoscenze acquisite durante lo svolgimento dell'intero corso. Il test è composto da 10 domande. L'esito finale dello stesso è considerato positivo se si risponde correttamente ad almeno l'80% delle domande.