enaip LOMBARDIA

IMAGINE LEARN LIVE

REGOLAMENTO PER UNA CORRETTA GESTIONE DEI DATI DELLE PERSONE FISICHE

In applicazione del Regolamento UE 2016/679 (GDPR) e del D. Lgs 196/2003

IMAGINE LEARN LIVE

UN ALTRO MODO PER VIVERE LA FORMAZIONE

1. REGOLE GENERALI

Le persone autorizzate al trattamento dei dati sono chiamate ad attenersi alle seguenti regole di ordinaria diligenza, che costituiscono il regolamento, nonché le altre misure ritenute necessarie per garantire il rispetto di quanto previsto in materia di protezione dei dati personali, sia per quanto riguarda i dati comuni (generali) che i dati particolari (sensibili).
Il Regolamento UE 2016/679 fa un elenco preciso dei dati particolari (sensibili):
essi sono i dati personali che rivelino:

- l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute, o alla vita sessuale o all'orientamento sessuale della persona, i dati giudiziari.

Tutte le persone autorizzate al trattamento dei dati sono impegnate alla riservatezza ed alla loro protezione. In particolare:

- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento delle finalità stabilite dalla Fondazione;
- tutte le operazioni di trattamento dovranno essere svolte garantendo il rispetto di misure di sicurezza e massima riservatezza;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro, si devono porre in essere tutte le misure necessarie (esempio blocco del pc con password, chiusura del fascicolo cartaceo) affinché soggetti terzi non possano accedere ai dati personali sia per i trattamenti automatizzati che cartacei;
- si richiede il massimo scrupolo nelle varie fasi di trattamento (raccolta, aggiornamento, conservazione, distruzione), soprattutto quando vengono trattate categorie particolari di dati;
- tali dati devono essere trattati secondo il principio della minimizzazione del trattamento, riducendo all'essenziale il loro utilizzo (evitare di salvare o stampare o duplicare documenti qualora non necessari all'attività lavorativa);
- le persone autorizzate a trattare categorie particolari di dati si dovranno attenere a specifiche istruzioni operative su come gestire i dati trattati con mezzi automatizzati e cartacei;
- le persone autorizzate debbono informare immediatamente un Responsabile del Trattamento qualora vi siano delle violazioni del Regolamento circa il trattamento dei dati personali e particolari.

2. SALVATAGGIO DATI

Tutti i dati al termine della giornata lavorativa vanno salvati nelle apposite aree aziendali messe a disposizione dalla Fondazione (server o spazio cloud).

- I dati non devono essere salvati sul desktop o sull'hard-disk del computer, sia perché ciò rappresenta un rischio per la sicurezza sia perché non possono essere salvati con backup.
- Occorre ricordare che se si utilizza un programma di posta elettronica, come Outlook, le mail e gli allegati vengono salvati normalmente sull'hard disk dell'computer, quindi sono maggiormente a rischio.

3. INTERNET E POSTA

Internet, posta elettronica e gli altri sistemi di messaggistica devono essere utilizzati esclusivamente per il lavoro. Al fine di poter garantire una sufficiente sicurezza, occorre attenersi alle seguenti regole:

- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, quali i dati particolari, senza garantire l'opportuna protezione;
- è opportuno evitare di utilizzare la posta elettronica (Outlook) come archivio principale nel quale conservare e ricercare i documenti; gli allegati, se contengono dati particolari, vanno scaricati e archiviati sul cloud o in cartelle di rete:

- è richiesta attenzione nell'invio di informazione e dati a destinatari di posta elettronica; dati personali vanno inviati solo a chi ha titolo per trattarli;
- al fine di minimizzare i dati da dover proteggere e gestire, è necessario cancellare messaggi e documenti inutili o allegati, se non più necessari (o non collegati con l'attività lavorativa).

4. ARCHIVI CARTACEI

I documenti cartacei vanno conservati in originale in archivi posti in luoghi non accessibili al pubblico, ad accesso controllato per persone preventivamente autorizzate. Le regole generali sono:
- i fascicoli ed i documenti che contengono dati personali non devono essere lasciati incustoditi nella postazione di lavoro e, terminato l'uso, devono essere conservati in un luogo sicuro;
- la persona autorizzata al trattamento dei dati non deve consentire l'accesso a terzi, se non autorizzati, anche quando il fascicolo o il documento è in lavorazione;
- in caso di trattamento di categorie particolari di dati tutta la documentazione cartacea deve essere conservata in armadi / cassetti o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro;
- debbono essere trattati nelle medesime modalità anche i dati "riservati", cioè quelli che riguardano la condizione familiare, la condizione economica, i cedolini paga, i dati bancari;
- le copie di documenti contenenti dati personali, quando non più necessarie devono essere o archiviate distrutte con qualunque mezzo che ne renda impossibile la ricostruzione; non possono essere utilizzate come carta da riciclo o da appunti;
- eventuali stampe di documenti, con stampanti di rete o sistema posti nell'ufficio, o documenti scansionati, non devono essere lasciati incustoditi ma prelevati al più presto dal vassoio di stampa o dalla cartella dello scanner e gestiti in modo controllato sulla propria scrivania o sul sistema informativo;
- in ogni caso va evitato di stampare o conservare copie di documenti contenenti dati particolari di persone fisiche; qualora fosse indispensabile, occorre sempre procedere alla loro distruzione fisica al termine delle lavorazioni.

5. SMART WORKING

La protezione dei dati delle persone fisiche è un obbligo anche durante il "lavoro agile", qualsiasi siano le modalità di lavoro e le tecnologie utilizzate. Protezione vuol dire che i dati devono essere utilizzati, gestiti ed archiviati in modo da ridurre i rischi di perdita, intrusione e furto. Le regole generali sono:
- di norma si opera accedendo ai dati conservati nella rete aziendale, sui server o in cloud;
- preferibilmente devono sempre essere utilizzati personal computer aziendali;
- nel caso si utilizzino, su autorizzazione, dei personal computer personali, questi debbono avere sistemi di protezione aggiornati (antivirus, firewall, ecc.);
- nel caso si faccia utilizzo di un personal computer non individuale (per esempio un computer ad uso promiscuo familiare), deve essere garantito un accesso con account personali che separino nettamente il loro utilizzo "aziendale" da quello familiare e soprattutto ad opera di altri utenti;
- le password personali vanno periodicamente aggiornate e modificate;
- i documenti in lavorazione, scaricati dal server o dal cloud, una volta chiusi, vanno salvati sempre sul server o sul cloud, senza tenerne copia sul personal computer in uso;
- non devono essere conservate copie cartacee dei documenti aziendali; se viene fatta una stampa di controllo, una volta controllato e salvato il documento digitale, la copia cartacea va distrutta ed eliminata in modo tale che non possa più essere ricostruita.

6. ACCESSI AI DATI DA PARTE DELL'AMMINISTRATORE DI SISTEMA (ADS)

L'amministratore di sistema è abilitato ad accedere ai dati di parte elettronica, esclusivamente in caso di necessità per motivi di sicurezza e protezione del sistema informatico in caso di necessità (ad esempio, virus, spyware, malware, intrusioni telematiche, spam, phishing), ovvero per motivi tecnici e/o di regolare svolgimento dell'attività aziendale.

- L'AdS è autorizzato ad intervenire sui dati per eseguire attività di ordinaria manutenzione di interventi urgenti.
- L'AdS, in caso di assenza improvvisa o prolungata del soggetto autorizzato o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica del soggetto autorizzato per le strette necessità operative.
- L'AdS può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, ad esempio mediante un sistema di controllo dei contenuti o mediante "file di log" della navigazione svolta.
- L'eventuale controllo sui file di log da parte dell'AdS non è comunque continuativo ed è limitato ad alcune informazioni - per esempio: per la posta elettronica (indirizzo del mittente/destinatario, data ed ora di invio/ricezione ed oggetto); per la navigazione internet (nome del soggetto autorizzato, identificativo dei device, indirizzo IP, data/ora di navigazione, siti visitati e totale accessi effettuati). I file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, fatti salvi in ogni caso specifici obblighi di legge.
- l sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente i dati personali degli utenti relativi agli accessi internet ed al traffico telematico. L'AdS è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti al soggetto autorizzato all'azienda per cessazione del rapporto sostituzione di apparecchiature ecc.
- Le verifiche sugli strumenti informatici saranno realizzate dall'azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente regolamento.

7. SANZIONI

Ogni persona autorizzata al trattamento dei dati, al fine di non esporre sé stesso e l'azienda al rischio di sanzioni, è tenuto ad adottare comportamenti conformi al presente regolamento ed è responsabile del corretto utilizzo degli strumenti aziendali e della sua condotta.
Il mancato rispetto del regolamento o la sua violazione potrà comportare provvedimenti di natura disciplinare o contrattuale, oltre ad azioni civili e penali laddove definiti dalle leggi.

8. CONTATTI

Le comunicazioni inerenti al trattamento e la protezione dei dati devono essere indirizzate a:
privacy@enaiplombardia.it
I responsabili interni del trattamento per la Fondazione Enaip Lombardia sono:
- Alessandro Tarpini: per i dati dei dipendenti, dei collaboratori, dei fruitori dei servizi al lavoro, degli utenti dei siti della Fondazione.
- Giuseppe Longhi: per i dati dei fruitori dei servizi formativi,
- Reti spa: Amministratore di Sistema

9. SOTTOSCRIZIONE

Il presente regolamento per una corretta gestione dei dati delle persone fisiche è stato predisposto dall'azienda, titolare del trattamento, ed è sottoscritto dal soggetto autorizzato, al quale ne è consegnata una copia, per presa visione ed accettazione del contenuto.

Nome Cognome	data	Firma per presa visione e accettazione
_____	_____	_____