

ALLEGATO N. 15

PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO, ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Premessa

Il presente piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'Ente;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui all'Art. 32 "Sicurezza di trattamento", del Regolamento UE 2016/679, in materia di protezione dei dati personali;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SGID o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;

- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, il Comune di Pray adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Sicurezza della rete di accesso al servizio

Il Sistema di Gestione Informatica dei Documenti del Comune di Pray non è esposto all'accesso attraverso la rete internet e non vengono utilizzati sistemi in cloud. Il sistema opera all'interno di un server installato nella rete LAN dell'Ente, ereditando dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione.

Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dall'allegato n. 2 al presente manuale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.

Le credenziali di autenticazione consistono in un codice (*User-Id*), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (*Password*), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'*User-Id* corrispondente, ma non la *Password* dello stesso.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della *Password*; quest'ultima è composta da almeno otto caratteri, tra cui almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare. La *Password* è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza mensile.

L'*User-Id* non può essere assegnato ad altri incaricati neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo secondo quanto stabilito dal presente manuale; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.

Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Gli incaricati del trattamento di dati personali, sensibili o giudiziari non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

Ai fini del trattamento dei dati personali, sensibili o giudiziari, sono impartite agli incaricati istruzioni scritte da parte del Responsabile per il trattamento dei dati personali, relative alle modalità delle operazioni, del controllo e della custodia di atti e documenti.

Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Formazione dei documenti

I documenti dell'AOO sono prodotti utilizzando i formati previsti dalla normativa.

Le risorse strumentali e le procedure utilizzate dal Comune di Pray per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'Amministrazione di riferimento
- la sottoscrizione dei documenti informatici con firma digitale ai sensi delle vigenti norme tecniche
- l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati nel sistema di protocollo informatico
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati
- la leggibilità e l'immodificabilità dei documenti nel tempo
- l'interscambiabilità dei documenti.

I documenti informatici prodotti dal Comune di Pray sono convertiti, prima della sottoscrizione con firma digitale, in formato PDF/A al fine di garantirne la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

La procedura di trasmissione alla firma del file PDF/A avviene mediante posta elettronica interna o aree di scambio tramite dischi di rete condivisi. La sottoscrizione con firma digitale del documento e degli eventuali allegati ne garantisce la titolarità e l'integrità.

La sottoscrizione del documento con firma digitale avverrà prima dell'effettuazione della registrazione di protocollo.

Sono utilizzati i diversi sistemi di validazione temporale elencati di seguito:

- il riferimento temporale contenuto nella segnatura di protocollo
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata
- l'utilizzo della marca temporale

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato alla protocollazione.

L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione dell'Ente; ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto, che gli sono stati assegnati o, comunque, di competenza del proprio ufficio di riferimento.

Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.

Eventuali modifiche, autorizzate ai sensi del presente manuale, vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnata da autorizzazione scritta del Responsabile della gestione documentale e il SGID deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.

L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente.

Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel manuale di conservazione, sarà trasferito, nell'arco della giornata lavorativa successiva, alla struttura di conservazione accreditata di cui l'Ente si serve, secondo quanto previsto nel presente manuale.

Gestione dei documenti e sicurezza logica del Sistema

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immutabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.

Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici in quanto la Siscom s.r.l. si impegna a rendere ragionevolmente sicuri gli accessi al Sistema e tutti i documenti e dati in esso contenuti tramite collegamento criptato (es. protocolli internazionali SSH, HTTPS).

Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti, vengono costantemente tenuti aggiornati, per mezzo dell'installazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

La Siscom garantisce la corretta esecuzione giornaliera delle copie dati che vengono effettuate automaticamente di notte.

Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti avviene secondo le direttive del Garante Privacy e più precisamente: il salvataggio dei dati e delle configurazioni del server. Il backup viene così effettuato con l'ausilio di procedure automatizzate:

Al termine dei backup, tutte le informazioni vengono salvate in un database per permettere ai responsabili delle copie di sicurezza di verificare il corretto funzionamento dei backup anche nei giorni successivi.

La visualizzazione dei log mostra, in una sola schermata, l'esito dei backup degli ultimi 7 giorni. E' quindi immediatamente visibile ogni eventuale anomalia (backup con errori, parziale o non effettuato).

Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici avviene entro 4 ore lavorative in caso di generico malfunzionamento, ed entro 12 ore lavorative in caso di disastro.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'Ente avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.

La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.

I messaggi di posta elettronica certificata prodotti dall'Ente sono compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD.

Conservazione dei documenti

I documenti registrati sul sistema di gestione documentale sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanente. Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel manuale di conservazione.

Il Piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal Comune di Pray siano disponibili, vengano conservati integri e riservati
- i dati personali (comuni, sensibili, giudiziari) siano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità per cui i dati sono stati raccolti, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Sicurezza fisica e infrastrutturale del Sistema

L'Ente, conformemente a quanto disposto dalla Circolare AgID n.1 del 17.03.2017 "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" dà attuazione agli adempimenti previsti dall'AgID.

In caso di perdita dei dati il servizio di Disaster Recovery prevede il ripristino degli stessi e dell'accesso ad essi entro 24 ore lavorative.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando un sistema di autenticazione basato su credenziali di accesso al pc utente e soprattutto con un'utenza applicativa personale. La profilazione degli utenti avviene in via preventiva e consente di definire le abilitazioni che possono essere attivate per ogni singolo utente o classi di utenti.

Il sistema di gestione documentale adottato dal Comune di Pray:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o classi di utenti
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente generico può accedere solamente ai documenti che gli sono stati direttamente assegnati o comunque ai documenti inviati al Servizio/i di appartenenza. Il Responsabile del Servizio può visualizzare tutti i documenti assegnati alle strutture di propria competenza.

Il sistema consente di associare un diverso livello di riservatezza per i documenti contenenti dati sensibili o giudiziari. I documenti non vengono mai visualizzati dagli utenti privi di diritto di accesso, neanche a fronte di una ricerca generale nel sistema informatico di gestione documentale.

Inoltre, grazie all'adozione di un *software* per la registrazione dei *Log-Access*, anche gli accessi degli Amministratori di Sistema sono monitorati e registrati da questo sistema di tracciamento.

Piani formativi del personale

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Il fornitore Siscom mantiene i log di sistema per 6 mesi, al fine di poter verificare eventuali violazioni del Sistema.

Il Responsabile della gestione documentale dell'ente effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.

Siscom, pertanto, tratterà i dati contenuti nei sistemi di sicurezza in modo da non eccedere le finalità per le quali gli stessi sono stati raccolti e solamente per il tempo strettamente necessario al conseguimento delle stesse; il trattamento dei dati dovrà impiegare modalità non invasive e attivare ogni possibile accorgimento finalizzato a salvaguardare la sfera privata altrui, come disposto dalla normativa vigente.

Gestione Data Breach

Premesse

L'Ente ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ateneo e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'Ente di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

Scopo

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati dall'Ente in qualità di Titolare del trattamento (di seguito "**Titolare del trattamento**"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

Cos'è una violazione dei dati personali

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- malware o virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

In pratica sono tutti quegli eventi che vanno a mettere a repentaglio gli elementi della sicurezza (DIR) in particolare:

- Disponibilità
 - distruzione
 - indisponibilità
 - perdita
- Integrità
 - alterazione
- Riservatezza
 - divulgazione
 - accesso

A chi sono rivolte queste procedure

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Destinatari esterni);

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

A quali tipi di dati si riferiscono queste procedure

Queste procedure si riferiscono a:

- dati personali trattati “da “e “per conto” del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

Per «dato personale» si intende: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Gestione comunicazione di data breach

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach da inviare a mezzo mail all'indirizzo privacy@labor-service.it oppure per mezzo PEC a pec@pec.labor-service.it DPO Comune di Pray : Labor Service S.r.l.

Gestione della violazione dei dati personali

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque step:

Step 1: Identificazione e indagine preliminare

Step 2: Contenimento, recovery e risk assessment

Step 3: Eventuale notifica all'Autorità Garante

Step 4: Eventuale comunicazione agli interessati

Step 5: Documentazione della violazione

Step 1: Identificazione e indagine preliminare

L'Allegato A, debitamente compilato, permetterà al Titolare del trattamento insieme al DPO, di condurre

una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento insieme al DPO dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso... ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'Allegato B - Modulo di valutazione del Rischio connesso al Data Breach che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, L'Ente dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento e il DPO invieranno la corretta modulistica all'Autorità Garante per

la protezione dei dati personali così da effettuare la notificazione del data breach.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, l'Ente sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta dell'Allegato C - Registro dei Data Breach, secondo le informazioni ivi riportate: (i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) se sia stata effettuata notifica all'Autorità Garante Privacy; (x) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo mail all'indirizzo privacy@labor-service.it oppure per mezzo PEC a pec@pec.labor-service.it
DPO Comune di Pray : Labor Service S.r.l.

Comunicazione di Data Breach	Note
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): In caso di destinatario esterno indicare la ragione sociale:	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile del dipartimento:	
data:	

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	A cura del DPO insieme con l'Ufficio IT e il Responsabile dell'ufficio coinvolto della violazione
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: operation, research, financial, legal, liability or reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	
<ul style="list-style-type: none"> o I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: <ul style="list-style-type: none"> a) origine razziale o etnica; b) opinion politiche, convinzioni religiose o filosofiche; c) appartenenza sindacale; d) dati genetici; e) dati biometrici; f) dati giudiziari; g) relative alla salute o all'orientamento 	

<p>sessuale di una persona.</p>	
---------------------------------	--

<p>o Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);</p>	
<p>o Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);</p>	
<p>o Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;</p>	
<p>Altro:</p>	
<p>La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?</p>	
<p>Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?</p>	
<p>Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)</p>	
<p>Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?</p>	
<p>Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?</p>	

Classificazione della violazione (1, 2 o 3) e motivazioni:	
Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)	Si/NO Se sì, notificato in data: Dettagli: