Disciplinare per l'utilizzo delle risorse strumentali informatiche e telematiche nell'ambito delle procedure di Screening COVID-19

Sommario

1 SCOPO DEL DOCUMENTO

Lo scopo del presente documento è fornire istruzioni sul trattamento dei dati personali al personale dipendente dell'ASL di Pescara e a tutti i soggetti coinvolti a vario titolo (ad es. Enti Locali e Associazioni di volontariato) nell'ambito delle attività di Screening Covid-19 a livello provinciale sia per la compilazione del data base unico fornito dalla ASL 03 Abruzzo.

2 DEFINIZIONI

Le seguenti definizioni sono utili per poter garantire la corretta esecuzione degli adempimenti ai quali è tenuto il Soggetto autorizzato al trattamento nell'ambito delle attività di cui al punto 1. In base all'art. 4 e all'art. 9 del Regolamento:

«dato personale»: 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;

"**dato personale appartenente a categorie particolari":** sono i dati che rivelino l'origina razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«violazione dei dati personali»: la violazione di sicurezza che comporta 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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«evento sulla sicurezza delle informazioni»: occorrenza identificata di uno stato di un sistema, servizio o della rete che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza

«incidente sulla sicurezza delle informazioni»: evento singolo o serie di eventi sulla sicurezza delle informazioni indesiderati o imprevisti che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni

«DPO»: Data Protection Officer o Responsabile della Protezione Dati

3 DIRETTIVE

3.1 Gestione documenti cartacei

Per la gestione dei documenti cartacei è necessario osservare le seguenti direttive:

- Limitare al massimo le stampe ove non indispensabili per motivi di lavoro (es.: firma di documenti)
- Distruggere qualsiasi documento lavorativo che non debba essere conservato (es.: documenti firmati) in maniera non ricostruibile
- In caso di stampa di documenti, conservarli in maniera da non renderli accessibili a persone non autorizzate.

3.2 Sicurezza dei Dati

Al fine di mettere in sicurezza i dati a cui l'utente ha accesso nell'ambito della propria autorizzazione sono raccomandate le seguenti misure:

- Cifratura dei dati sui dispositivi (soprattutto mobili) e dei supporti su cui eventualmente vengano copiate le informazioni (es.: chiavette USB, dischi esterni, ecc…) ove autorizzate.
- Backup dei dati secondo quanto indicato dal proprio servizio di assistenza tecnica
- Assicurarsi che i dati temporaneamente elaborati sui propri dispositivi siano da questi effettivamente cancellati dopo averli salvati sulle infrastrutture aziendali.

3.3 Utilizzo e conservazione dei supporti rimovibili

Devono essere osservate le seguenti direttive:

- In linea generale, i supporti di memorizzazione removibili (es. hard disk esterni, CD/DVD, pendrive usb, ecc), contenenti dati personali, non possono essere utilizzati.
- Nei casi previsti ed autorizzati dal proprio responsabile, i supporti removibili, contenenti dati personali devono essere adeguatamente custoditi, possibilmente in cassetti e armadi provvisti di chiusura e devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o recuperato successivamente alla cancellazione.
- A tal proposito si ricorda che il soggetto autorizzato è responsabile non solo della custodia dei supporti ma anche dei dati in essi contenuti.
- Nel caso di riutilizzo condiviso dei medesimi supporti da parte di più utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante specifici programmi.

3.4 Politica di schermo e scrivania puliti

Oltre a quanto già esplicitamente previsto nel presente documento è necessario osservare le seguenti disposizioni:

- Riporre, a fine giornata o nelle pause prolungate, i documenti ed i supporti informatici rimovibili, se autorizzati, che contengono dati personali e/o particolari nei cassetti o negli armadi (preferibilmente chiusi a chiave).
- Le chiavi degli archivi e dei cassetti non devono essere lasciate incustodite.
- Nel caso in cui l'utente abbia a disposizione un PC portatile aziendale, alla fine della giornata lavorativa il dispositivo deve essere riposto in luogo chiuso (es.: cassetto o armadio) o, in caso di necessità del dispositivo anche al di fuori del luogo di lavoro, averne cura per tutta la durata dell'utilizzo.
- In caso ci si allontani dal pc, bloccare il pc in modo che non sia utilizzabile da altri (attivare il blocco schermo);
- Non consentire a personale non esplicitamente autorizzato di visualizzare le informazioni a cui si ha accesso;
- Non lasciare incustodite le credenziali con password per accedere ai file allegati alle email, agli applicativi, alla rete aziendali;
- Non effettuare foto, "print screen" o cattura dello schermo nel corso di una sessione di lavoro o quando si ha accesso ad informazioni e dati per motivi di lavoro;
- Stampe contenenti informazioni riservate o sensibili devono essere immediatamente rimosse dalla stampante;

- Distruggere i documenti, quando non più necessari, rendendoli illeggibili. Ricorrere, ove possibile, all'utilizzo del trituratore, impedendo, comunque, la visibilità dei documenti a persone non esplicitamente autorizzate;
- Le lavagne contenenti informazioni riservate devono essere opportunamente cancellate dopo l'utilizzo e comunque le informazioni in esse indicate non devono essere accessibili a personale non autorizzato.

3.5 Ulteriori Misure di sicurezza

Per un efficace protezione dei dati personali, si invita tutto il personale ad osservare le seguenti istruzioni:

- Non trasmettere o divulgare a terzi i dati personali, tramite supporti informatici o altri mezzi (es. posta, e-mail, fax, social network, etc..), senza la previa autorizzazione del proprio responsabile/supervisore.
- Evitare di proteggere file contenenti dati personali e/o particolari ad utilizzo lavorativo tramite password di file di propria esclusiva conoscenza.
- Riprodurre i dati (creando copie degli archivi, fotocopiando documenti, etc.) per le proprie esigenze lavorative solo se è strettamente necessario e, comunque, rispettando i criteri di sicurezza validi per i dati/documenti originali;
- L'autorizzato al trattamento dei dati che preleva dati personali/cartacei deve, durante la propria attività, preservarli da accessi non autorizzati e riporli in archivio a fine lavoro;
- Procedere alla cancellazione/distruzione delle copie di dati riprodotte non appena possibile al fine di evitare la proliferazione incontrollata di archivi contenenti dati personali e/o particolari;
- Garantire adeguata custodia dei documenti e dei supporti informatici che contengono dati personali anche all'esterno della sede dell'organizzazione (Azienda) (ad es. in viaggio, ecc.);
- Utilizzare per la stampa apparecchiature collocate in aree controllate. Quando non disponibili, presidiarle in fase di stampa;
- Le chiavi delle porte e degli armadi che regolano l'accesso agli archivi di dati particolari dovranno essere custodite dagli autorizzati referenti delle aree o da persone da questi delegate e potranno essere richieste solo ed esclusivamente dal personale autorizzato.

4 DATA BREACH

Nel caso in cui un Soggetto Autorizzato al Trattamento dei Dati si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il dr Rossano Di Luzio (Soggetto Autorizzato al Trattamento con Delega) della possibile violazione. Quest'ultimo dovrà quindi informare l'Ufficio Privacy, l'UOSD Sistemi Informativi ed il Responsabile Protezione Dati (DPO)

FINE DOCUMENTO