ISTITUTO
DEGLI INNOCENTI

ISTRUZIONI OPERATIVE PER GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Direttiva del Direttore generale
n. 1/2023

Istituto degli Innocenti

ISTITUTO DEGLI INNOCENTI

ISTRUZIONI OPERATIVE PER GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Direttiva del Direttore generale n. 1/2023

www.istitutodeglinnocenti.it

ISTITUTO DEGLI INNOCENTI

ISTRUZIONI OPERATIVE PER GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Direttiva del Direttore generale n. 1/2023

Sommario

50122 Firenze, Italia
Piazza SS.Annunziata, 12
centralino tel.055.20371
fax 055.241663

1. Scopo

Il presente documento risponde alle indicazioni del Regolamento europeo sulla protezione dei dati 2016/679 (GDPR) con particolare riferimento all'art. 28 punto 3, e all'art. 29 che richiedono che qualsiasi persona "autorizzata al trattamento dei dati personali" sia debitamente informata ed istruita al fine di mettere in atto comportamenti che assicurino l'adeguato livello di sicurezza e riservatezza commisurato al "valore del dato" e ai conseguenti rischi.

2. Premessa

Al fine di rispondere all'esigenza di informazione ed istruzione delle persone autorizzate al trattamento di dati personali dell'Istituto degli Innocenti (sia in qualità di titolare che di responsabile del trattamento), il seguente documento si riferisce agli aspetti generali di comportamento ed attenzione che devono essere adottati nello svolgimento delle attività di competenza di ciascuno. Le istruzioni specifiche, relative al trattamento/ai trattamenti per i quali la persona viene autorizzata, esulano dal presente documento e sono impartite a cura del titolare/responsabile o suo delegato.

L'autorizzazione al trattamento di dati personali avviene in maniera esplicita, da parte del titolare/responsabile, con specifica lettera di nomina indicante:

- la persona autorizzata;
- i trattamenti di dati personali a cui si è autorizzati e censiti nel registro dei trattamenti;
- l'informativa privacy per il soggetto autorizzato.

Le istruzioni generali contenute nel presente documento completano il quadro informativo fornito ai soggetti autorizzati sui comportamenti da tenere al fine di assicurare adeguati livelli di sicurezza e riservatezza.

3. Istruzioni generali per le persone autorizzate al trattamento dei dati personali

In ottemperanza alle disposizioni della normativa sulla protezione dei dati personali ed in relazione alle attività svolte nell'ambito della struttura organizzativa in cui opera, la persona autorizzata al trattamento dei dati personali dovrà effettuare i trattamenti dei dati di competenza nel rispetto dei seguenti principi:

- consapevolezza e responsabilizzazione del "valore" dei dati trattati;
- osservanza e obbligo dei criteri di riservatezza;
- liceità e correttezza;

- rispetto delle misure di sicurezza;
- custodia e controllo dei dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di divulgazione o accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure di sicurezza in relazione agli obblighi di cui all'art. 32 del Regolamento 2016/679/UE (di seguito GDPR), sono, nel seguito e per maggior chiarezza, distinte in funzione delle seguenti modalità di trattamento dei dati:

- senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
- con strumenti elettronici (PC e o altri sistemi IT).

3.1 Trattamenti senza l'ausilio di strumenti elettronici

I supporti di tipo magnetico e/o ottico, contenenti dati personali, devono essere protetti dal punto di vista fisico con le misure di sicurezza analoghe a quelle previste per i supporti cartacei.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali e commisurate al valore del dato.

Il "valore del dato" è costituito da una valutazione della tipologia di dati trattati (comuni, particolari, giudiziari), dalle categorie e dalla numerosità degli interessati.

3.1.1 Custodia

I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili alle persone non autorizzate al trattamento dei dati stessi (es. armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

I documenti contenenti dati personali non devono rimanere incustoditi sulle scrivanie o tavoli di lavoro.

3.1.2 Comunicazione

L'utilizzo dei dati personali deve essere limitato alle informazioni di cui la persona autorizzata ha necessità di accedere per lo svolgimento dei compiti assegnati (principio del need to know). I dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività lavorative (anche se queste persone sono a loro volta persone autorizzate al trattamento dei dati personali).

I dati non devono essere comunicati all'esterno dell'Ente e comunque a soggetti terzi, se non previa autorizzazione.

3.1.3 Distruzione

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

3.1.4 Istruzioni in caso di trattamento di categorie di dati personali particolari o giudiziari

I documenti contenenti categorie particolari di dati personali (di seguito "dati particolari"), dati relativi a condanne penali e reati (di seguito "giudiziari"), devono essere controllati e custoditi in modo che non vi possono accedere persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in applicazioni IT di gestione/amministrazione del personale, (es. dati relativi a permessi sindacali, assenze per malattie ecc.), deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

3.2 Trattamenti di dati personali con l'ausilio di strumenti elettronici

3.2.1 Gestione delle credenziali di autenticazione

L'accesso alle applicazioni IT che trattano dati personali, è consentito alle persone autorizzate in possesso di "credenziali di autenticazione" (profilo di accesso) che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione delle persone autorizzate al trattamento dei dati personali (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card, badge, tessera sanitaria, sistemi a due o più fattori, ecc.). Le persone autorizzate al trattamento dei dati personali, devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- le user-id e relativa password per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se autorizzati al trattamento);
- nel caso altri utenti debbano poter accedere ai dati è necessario che gli stessi siano registrati come autorizzati e che venga loro assegnata una credenziale;
- le credenziali di autenticazione (ad esempio le password, oppure i dispositivi di strong authentication come token, smartcard ecc.) che consentono l'accesso alle

applicazioni devono essere mantenute riservate. Esse non vanno mai condivise con altri utenti (anche se persone autorizzate al trattamento dei dati personali);
- le password devono essere sostituite, a cura della persona autorizzata al trattamento dei dati personali, al primo utilizzo e successivamente secondo le indicazioni fornite dal settore competente in materia di sicurezza IT;
- le password devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- le password non devono contenere riferimenti agevolmente riconducibili alla persona autorizzata al trattamento dei dati personali (es. nomi di familiari, data di nascita, ecc.) e devono essere scelte nel rispetto delle eventuali indicazioni dell'ente sulla costruzione ed utilizzo delle password (vedi anche successivo punto).

Qualora il sistema preveda più strumenti di autenticazione, l'autorizzato deve scegliere quello maggiormente sicuro fra quelli a sua disposizione.

3.2.2 Istruzioni specifiche per la gestione delle credenziali di strong authentication

In caso in cui l'accesso ai sistemi e alle applicazioni IT avvenga tramite sistemi di autenticazione "robusta" (strong authentication), la persona autorizzata al trattamento dei dati personali deve attenersi alle seguenti specifiche istruzioni per quanto riguarda la gestione delle proprie credenziali e dispositivi di autenticazione:

- i dispositivi di strong authentication (es. token, smart card, ecc.) devono essere conservati con cura, per evitare furti o smarrimenti;
- il codice personale (PIN) deve essere modificato direttamente dalla persona autorizzata al trattamento dei dati personali al primo accesso e successivamente almeno ogni sei mesi o secondo una periodicità definita dal responsabile della sicurezza. Inoltre, il PIN non deve essere rivelato ad alcuno e va custodito in maniera tale da evitare che altri possano venirne a conoscenza;
- la persona autorizzata al trattamento dei dati personali deve segnalare prontamente ogni fatto anomalo (es. furto, smarrimento, ecc.) riguardante i propri dispositivi di autenticazione tramite presentazione di una dichiarazione sostitutiva di atto notorio rivolta all'amministrazione o mediante denuncia alle autorità competenti, qualora previsto espressamente dalla normativa;

- i dispositivi di strong authentication rilasciati dall'Istituto e collegati alla funzione svolta all'interno dell'ente devono essere riconsegnati quando non sono più necessari per lo svolgimento della stessa (ad esempio per cambio mansione), oppure al termine del rapporto di lavoro.

3.3 Protezione del PC e dei dati

Tutti i PC devono essere dotati di password rispondenti alle normative e linee guida vigenti.
Le password devono essere custodite e gestite come previsto dalle indicazioni aziendali, ivi compresa la loro sostituzione periodica.
In caso di prolungata assenza della persona autorizzata al trattamento dei dati personali o di dimissioni della stessa e solo per urgenti ed indifferibili necessità di lavoro che richiedano l'accesso alla messaggistica, che non possano essere espletate con altre modalità, il Direttore responsabile o il Direttore generale invierà al servizio responsabile per i sistemi IT/amministratore del sistema di autenticazione, una richiesta di reset della password di accesso al profilo personale e alla casella di posta elettronica aziendali della persona autorizzata al trattamento dei dati personali assente.

Eseguita l'operazione di reset password, l'amministratore del sistema di autenticazione, comunicherà la nuova password (non tramite posta elettronica) al richiedente e al contempo invierà una comunicazione alla persona autorizzata al trattamento dei dati personali assente. Solo nei casi in cui il reset della password non possa essere applicato, le password di accesso devono essere consegnate in busta chiusa al richiedente per le finalità e con le modalità di cui al presente paragrafo.

Tutti i PC devono essere dotati di software antivirus distribuito e aggiornato costantemente da parte degli amministratori di tali *assets*.

Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dall'Istituto. Sono vietati i software scaricati da Internet o acquisiti autonomamente. Qualora se ne manifestasse la necessità per compiti di ufficio occorre darne comunicazione alla PO di appartenenza che autorizzerà l'eventuale acquisto e successivamente al servizio responsabile per i sistemi IT che, rilascerà, invece, il parere tecnico.

Per evitare accessi illeciti, deve essere sempre attivato il salvaschermo con password.

Sui PC devono essere installati, secondo le procedure previste e appena vengono resi disponibili e sono approvati dall'Ente, tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

Qualora per esigenze d'ufficio si dovesse procedere a scaricare sul PC d'ufficio o su supporti removibili dati personali da procedure on line centralizzate, si ricordi che questo costituisce Trattamento di dati personali che come tale dovrà essere gestito nei limiti dell'autorizzazione.

3.4 Cancellazione dei dati dai PC

Occorre che l'utente cui è assegnato il PC abbia consapevolezza del "valore dei dati personali" archiviati sull'archivio locale del PC come degli eventuali archivi di rete o supporti removibili.
I dati personali conservati sui PC devono essere cancellati in modo sicuro, scegliendo la modalità più idonea al valore di dati archiviati, prima di destinare i PC ad usi diversi. Sia in caso di cambio PC che dismissione utente l'attività di pulizia verrà eseguita dal servizio responsabile per i sistemi IT.

4. Istruzioni di carattere generale

4.1 Come comportarsi in presenza di ospiti o di personale di servizio

Alcune regole o comportamenti al fine di evitare rischi nella normale attività lavorativa con altre persone:

- fare attendere gli ospiti in luoghi in cui non siano presenti dati riservati o dati personali;
- se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti attivare il salvaschermo con password del PC;
- non rivelare o fare digitare le proprie password dal personale di assistenza tecnica o da altri colleghi;
- non rivelare le password al telefono, nessuno è autorizzato a chiederle, né inviarle per posta elettronica;
- segnalare qualsiasi anomalia o stranezza al servizio responsabile per i sistemi IT;
- non lasciare incustoditi i propri strumenti di autenticazione forte (es. tessera sanitaria, badge, ecc.).

4.2 Come gestire la posta elettronica

Per la gestione della posta elettronica e dei servizi di occorre porre particolare attenzione a:

- non aprire, in nessun caso, messaggi con allegati di cui non si conosce l'origine (possono contenere virus in grado di alterare i dati sul PC, installare virus, criptare i dati rendendoli non più accessibili, ecc.);
- per lo stesso motivo di cui al punto precedente, evitare, nel modo più assoluto, di aprire filmati e presentazioni scherzose, possono essere pericolose per i dati contenuti nel PC o rete aziendale;
- evitare l'inoltro automatico dalla propria casella dell'Ente verso caselle personali esterne;
- cancellare tutti i messaggi dei quali non si conosce la fonte o si hanno sospetti. In particolare tenuto conto dell'aumento degli attacchi basati su ingegneria sociale si

ricorda che MAI arrivano avvisi di pagamento o altro a mezzo email ordinarie, ma SOLO tramite PEC.

- si raccomanda, pertanto, di eliminare tutto quanto arrivi con le caratteristiche sopra indicate, soprattutto se con allegati. In caso di dubbi è possibile chiedere una verifica preliminare al servizio responsabile per i sistemi IT.

4.3 Come usare correttamente Internet

Per la gestione dei servizi Internet, dei social ecc. si faccia riferimento a quanto di seguito riportato, oltre che alle previsioni del Codice di comportamento dei dipendenti dell'Istituto, consultabile nella sezione Amministrazione trasparente del sito aziendale. In particolare si invita a:

- evitare di scaricare software da Internet (programmi di utilità, di *office automation*, file multimediali, ecc.), in particolare se non se ne conosce l'attendibilità della sorgente, in quanto questo può essere pericoloso per i dati e la rete aziendale. I software necessari all'attività lavorativa vanno richiesti ai competenti riferimenti istituzionali come sopra individuati;
- usare Internet entro i limiti consentiti dalle procedure/regolamenti dell'ente, i siti web spesso nascondono insidie per i visitatori meno esperti;
- evitare l'iscrizione a gruppi o altro di cui non si conosce l'affidabilità della sorgente.

4.4 Utilizzo di supporti removibili

L'utilizzo di supporti removibili (chiavette USB, dischi USB, ecc.) deve essere limitato alle effettive necessità. Nel caso di dati personali con maggiore attenzione a quelli particolari o giudiziari, è da evitare per qualsivoglia motivo la loro archiviazione su supporti removibili.

In caso di perdita o furto occorre immediatamente darne comunicazione al proprio Dirigente e al DPO, per le valutazioni del caso a norma del GDPR.

4.5 Utilizzo di servizi di produttività personale in Cloud

L'utilizzo di servizi in Cloud con particolare riferimento a quelli di utilità personale (agenda, contatti, repository di cartelle e file, ecc..), non regolati da specifico contratto fra l'Ente e il fornitore dei servizi (tipicamente quelli gratuiti, es. Gdrive, Drop Box, ecc.) sono da evitare e sono vietati se il loro uso coinvolge dati personali di titolarità dell'Istituto degli Innocenti o di cui l'Istituto è responsabile del trattamento. Nel caso di impellenti necessità e in caso di non disponibilità di altri strumenti idonei è necessario rivolgersi al servizio responsabile per i sistemi IT per l'autorizzazione e corrette istruzioni di utilizzo.

50122 Firenze, Italia
Piazza SS.Annunziata, 12
centralino tel.055.20371
fax 055.241663

4.6 Come comportarsi in caso di violazioni di sicurezza

In caso di eventi relativi a possibili violazioni di dati personali o di incidente di sicurezza (c.d. data breach), costituiti a titolo esemplificativo da:

- distruzione di dati digitali o documenti cartacei,
- perdita di dati conseguente a smarrimento/furto di supporti o di documentazione,
- rilevamento di modifica non autorizzata di dati,
- divulgazione di dati e documenti a soggetti terzi non legittimati,
- accesso non autorizzato a sistemi IT, ecc.

In caso di possibili incidenti di sicurezza, occorre informare prontamente il proprio dirigente/responsabile di servizio e il servizio responsabile per i sistemi IT al fine dell'attuazione degli adempimenti previsti in applicazione delle disposizioni di legge.

5. Informazioni

Ulteriori informazioni e approfondimenti sono disponibili nell'intranet aziendale, sezione Direzione Generale/ "Privacy – Trattamento dei dati"

Il Direttore generale
Sabrina Breschi

Documento firmato da:
BRESCHI SABRINA
19.01.2023 13:04:31
UTC