Giunta regionale toscana

Istruzioni per gli autorizzati
Disciplinare

Indice

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, il seguente documento si riferisce agli aspetti generali di comportamento ed attenzione che devono essere adottate nello svolgimento delle attività di competenza di ciascuno. Le istruzioni specifiche, relative al trattamento o ai trattamenti per i quali la persona viene autorizzata e conseguentemente censita nel registro dei trattamenti, esulano dal presente documento e sono compito del titolare/responsabile o suo delegato impartire.
L'autorizzazione al trattamento di dati personali avviene in maniera esplicita da parte del titolare o suo delegato (dirigente del settore competente nella materia)[1], indicando:

1. La persona autorizzata,
2. I trattamenti di dati personali a cui si è autorizzati, censiti nel registro dei trattamenti,
3. L'applicazione IT (laddove esistente) e il relativo profilo di accesso, e/o l'archivio cartaceo
4. Le istruzioni generali facendo riferimento al presente documento,
5. Eventuali istruzioni specifiche.

Nota bene: Nel caso di autorizzazioni da parte dei settori regionali che operano come "Responsabili" per altri enti, valgono le stesse istruzioni del presente documento, rendendo edotte le persone, gli autorizzati, che trattano dati di altri titolari.

1 Il personale dipendente e i soggetti che vi operano ad altro titolo, che agiscono l' autorità dei dirigenti regionali, ad oggi è stato autorizzato ed istruito al trattamento dei dati personale con DGR 585/2018 (Allegato 1 "Istruzioni al trattamento dei dati personali")

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 (direzione o settore) in cui opera, la persona autorizzata al trattamento dei dati personali, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle istruzioni contenute nel presente documento e ad ogni ulteriore indicazione, fornita dal Titolare/Responsabile o da suo delegato.
I comportamenti messi in atto nell'esercizio delle funzioni, debbono conformarsi ai seguenti principi:

1. consapevolezza e responsabilizzazione del "valore" dei dati trattati;
2. osservanza e obbligo dei criteri di riservatezza;
3. liceità e correttezza;
4. rispetto delle misure di sicurezza;
5. 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 previste dalle policy della Regione Toscana in relazione agli obblighi di cui all'art. 32 del Regolamento 2016/679/UE (di seguito GDPR) sono per maggior chiarezza distinte in funzione delle seguenti modalità di trattamento dei dati:

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

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

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 avvenire in base al principio del "need to know" e cioè essi 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 accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di 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.
Per accedere agli archivi contenenti dati particolari e giudiziari fuori orario di lavoro è necessario farsi identificare e registrare sugli appositi registri.

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

3.2.1 Gestione delle credenziali di autenticazione

L'accesso alle procedure informatiche 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..) o in una caratteristica biometrica.
Le persone autorizzate al trattamento dei dati personali devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

1. Le user-id e relativa password per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se autorizzati al trattamento);
2. 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
3. Le credenziali di autenticazione (ad esempio le password, oppure i dispositivi di strong authentication come token, smart card 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).
4. Le password devono essere sostituite, a cura della singola persona autorizzata al trattamento dei dati personali, al primo utilizzo e successivamente almeno ogni tre mesi, salvo modalità e periodi, stringenti o più rilassati, di volta in volta comunicati formalmente dai responsabili della sicurezza IT o previsti da specifiche procedure o misure di sicurezza.
5. 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 della politica dell'ente sulla costruzione ed utilizzo delle password (vedi anche successivo punto).

6. 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 di trattamento di dati particolari o giudiziari, l'accesso ai sistemi e alle applicazioni IT deve avvenire tramite sistemi di autenticazione "robusta" (strong authentication). In questi casi, nonché in tutti gli altri eventuali casi in cui è prevista la strong authentication per accedere ai sistemi, oltre a quanto indicato nelle altre sezioni delle presenti istruzioni, 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:

1. I dispositivi di strong authentication (es. token, smart card, ecc..) devono essere conservati con cura, per evitare furti o smarrimenti.
2. 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. Inoltre, il PIN non deve essere rivelato ad alcuno e va custodito in maniera tale da evitare che altri possano venirne a conoscenza.
3. La persona autorizzata al trattamento dei dati personali deve segnalare prontamente ogni fatto anomalo (es. furto, smarrimento, ecc.) riguardante i propri dispositivi di autenticazione con le modalità previste dall'ente, tramite presentazione di una dichiarazione sostitutiva di atto notorio rivolta all'amministrazione o mediante denuncia alle autorità competenti, qualora previsto espressamente dalla normativa.
4. I dispositivi di strong authentication devono essere riconsegnati quando non sono più necessari per svolgere l'attività lavorativa (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 relative normative aziendali, ivi compresa la loro sostituzione periodica.
In caso di prolungata assenza della persona autorizzata al trattamento dei dati personali, solo per urgenti ed indifferibili necessità di lavoro che non possano essere espletate con altre modalità, il dirigente responsabile invierà una mail di richiesta di reset della password del PC della persona autorizzata al trattamento dei dati personali assente, all'amministratore del sistema di autenticazione o altra funzione competente di riferimento. Eseguita l'operazione di reset password, l'amministratore del sistema di autenticazione, comunicherà la nuova password al dirigente e al contempo invierà una email informativa 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 ai PC contenenti dati personali, nonché le eventuali password per l'accesso ai singoli file contenenti tali dati, devono essere consegnate in busta chiusa al dirigente per le finalità e con le modalità di cui alla normativa dell'ente.
Tutti i PC devono essere dotati di software antivirus distribuito e aggiornato costantemente da parte degli amministratori di tali Asset.
Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dall'Azienda. Sono vietati i software scaricati da Internet o acquisiti autonomamente. Qualora se ne manifestasse la necessità per compiti di ufficio occorre darne comunicazione al dirigente responsabile delle dotazioni tecnologiche degli uffici della Regione Toscana.
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 proprio PC o su supporti removibili dati personali da procedure on line centralizzate, si ricordi che questo costituisce Trattamento di Dati personali che deve essere registrato nell'apposito registro indicando come asset il proprio PC.
Il trattamento di dati personali, attraverso programmi di produttività installati sul proprio PC deve essere presente nel registro dei trattamenti.

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. Questa attività deve essere assistita da un addetto con specifiche competenze e ruolo all'interno dell'ente.

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:

1. Fare attendere gli ospiti in luoghi in cui non siano presenti dati riservati o dati personali.
2. Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo con password del PC, (premendo ctrl-alt-canc).
3. Non rivelare o fare digitare le proprie password dal personale di assistenza tecnica o da altri colleghi.
4. Non rivelare le password al telefono - nessuno è autorizzato a chiederle, né inviarle per posta elettronica,
5. Segnalare qualsiasi anomalia o stranezza al Data Protection Specialist della Direzione.
6. 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 collaborazione si segua quanto definito nell'apposito disciplinare. Fra le altre cose occorre porre particolare attenzione a:

1. 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..
2. 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 sul vostro PC.
3. Evitare l'inoltro automatico dalla propria casella dell'ente verso caselle personali esterne.
4. Cancellate tutti i messaggi dei quali non conoscete la fonte o avete sospetti.

4.3 Come usare correttamente Internet

Per la gestione dei servizi internet, dei social ecc.. si faccia riferimento al relativo disciplinare e in particolare:

1. 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 alle competenti funzioni aziendali.
2. Usare Internet entro i limiti consentiti dalle procedure/regolamenti dell'ente, i siti web spesso nascondono insidie per i visitatori meno esperti.
3. Non leggere le caselle personali esterne via webmail, in quanto i provider esterni potrebbero non proteggere dai virus.
4. 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. Qualora l'utilizzo di supporti removibili non possa essere evitato è obbligatorio cifrare i dati in esso contenuti e distruggerli dopo il loro utilizzo. Le chiavi di cifratura e la loro conservazione, debbono seguire regole che garantiscano la sicurezza e riservatezza del dato.
In caso di perdita o furto occorre immediatamente ricorrere al security manager dell'ente 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.*** Nel caso di impellenti necessità e in caso di non disponibilità di altri strumenti idonei occorre coinvolgere nell'utilizzo di questi strumenti il Security Manager.

5 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:

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

In caso di possibili incidenti di sicurezza, occorre informare prontamente il proprio dirigente di settore e coinvolgere il Security Manager al fine dell'attuazione degli adempimenti previsti in applicazione delle disposizioni di legge.

6 Data Protection Policy – Regione Toscana

Le disposizioni di legge sulla protezione dei dati personali in ottemperanza a quanto stabilito dal regolamento UE 2016/679, (GDPR) sono illustrate nel documento "Data Protection Policy" pubblicato sul sito http://www.regione.toscana.it/data_protection_officer/.

7 Obbligo di osservanza delle istruzioni

Tutti gli autorizzati sono chiamati ad applicare ed attenersi scrupolosamente alle presenti istruzioni, impartite ai sensi delle normative vigenti in materia di trattamento dei dati personali.

8 Facs- simile Autorizzazione

Premesso che con DGR 585/2018 si è provveduto a fornire l'autorizzazione generale in base alle competenze di ogni singolo addetto, l'autorizzazione di una persona ad un trattamento, sia che avvenga con modalità e procedure digitali sia in altro modo, deve contenere i seguenti dati:

Ente _____
Il titolare/responsabile o suo delegato _____

Il sig/ra _____
È autorizzata, a norma del GDPR, ai seguenti trattamenti con relativi profili di accesso (funzioni)

Nome e numero trattamento	Funzioni/profili di accesso
_____	_____
_____.	_____
_____.	_____

.
.

L'autorizzato/a è tenuto/a, a norma del GDPR ad assicurare il massimo livello di riservatezza nel trattamento di dati personali e a seguire le misure comportamentali e di sicurezza adeguate con particolare riferimento a quanto indicato nel disciplinare di istruzione agli Autorizzati presente nella intranet sezione relativa alla protezione dei dati personali.

Il Titolare/Responsabile. F.to. _____

Per presa visione

L'autorizzato/a F.to _____

Nota bene: *Nel caso di autorizzazioni da parte dei settori regionali che operano come "Responsabili" per altri enti, valgono le stesse istruzioni del presente documento, rendendo edotte le persone, gli autorizzati, che trattano dati di altri titolari.*