Appendice al CODICE DI COMPORTAMENTO DEI DIPENDENTI
Approvato con Deliberazione della Giunta dell'Unione n° 87 del 15/09/2017

UNIONE DEI COMUNI DELLA VAL D'ENZA
NORME DI COMPORTAMENTO FINALIZZATE ALLA PROTEZIONE DEI DATI PERSONALI

Premessa

Il Regolamento Europeo sulla protezione dei dati personali prescrive che questi ultimi siano trattati in modo tale da garantire una loro adeguata protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

La protezione dei dati personali comprende le misure sia informatiche che fisiche delle aree e dei locali, degli strumenti elettronici utilizzati per il trattamento e degli archivi cartacei, degli atti e dei documenti contenenti dati personali.

Si riportano di seguito alcune norme di comportamento che devono essere applicate da chi, all'interno dell'organizzazione, tratta dati personali, così come definiti dal Regolamento Europeo ("qualsiasi informazione riguardante una persona fisica identificata o identificabile") e la cui modalità di gestione è rappresentata nei registri della attività di trattamento.

Regola dello 'schermo sicuro'

Chiunque tratti a qualunque titolo dati personali all'interno dell'ente non lascia incustodito e accessibile lo strumento elettronico utilizzato durante il trattamento; in caso di assenza temporanea, termina la sessione di trattamento o attiva il blocco con parola chiave dello strumento (Screen Saver protetto con Password).

Regola della 'scrivania sicura'

Chiunque tratti a qualunque titolo dati personali all'interno dell'ente, nello svolgimento delle operazioni di trattamento, controlla e custodisce con cura gli atti e i documenti contenenti dati personali in modo che ad essi non possano avere accesso persone prive di autorizzazione, conservandoli negli appositi archivi al termine delle operazioni –se fisici possibilmente chiusi a chiave.

Protezioni rinforzate per i dati relativi a condanne penali e reati e i dati sanitari e genetici

Gli archivi cartacei contenenti dati relativi a condanne penali e reati sono conservati in armadi dotati di serratura o in aree o locali ad accesso controllato. Il prelievo di documenti da tali archivi deve essere indicato su un apposito registro. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, sono identificate e registrate.
Le strutture dell'ente che trattano questi dati adottano misure tecniche e/o organizzative per la cifratura dei dati sensibili e altre misure preventive (es., pseudonimizzazione) al fine di consentire il trattamento disgiunto dei medesimi dagli altri dati personali che permettono di identificare direttamente gli interessati.

Aggiornamento del software e dei sistemi antivirus

Il Servizio Informatico Associato dell'Unione cura gli aggiornamenti periodici dei software di base e applicativi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono effettuati con la massima tempestività e possibilmente con strumenti automatici di controllo delle configurazione.
E' vietata a tutti i dipendenti l'installazione di applicativi software non preventivamente autorizzati dai servizi informatici dell'Ente.

Gli strumenti elettronici che contengono dati personali sono protetti contro il rischio di intrusione tramite installazione di s*istemi antivirus* aggiornati in modo automatico.

Backup dei dati personali

Tutti i sistemi in cui sono memorizzati dati personali sono sottoposti a procedure automatiche di backup, come nelle policy specifiche del SIA sulle modalità e gestione servizi di back up, tali da garantire il recupero dei dati – almeno del giorno precedente - a fronte della cancellazione o modifica non autorizzata o prevista dei dati o anche della distruzione fisica o furto del sistema.

Gestione dell'accesso ai dati personali

L'accesso ai dati personali conservati informaticamente prevede specifiche misure di controllo per tracciare e limitare l'accessibilità ai soli autorizzati e incaricati.
La parola chiave (Password), prevista dal sistema di autenticazione informatica e utilizzata da chi tratta dati personali deve:

- essere composta da almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- includere almeno un carattere maiuscolo ed almeno una cifra numerica e possibilmente almeno un carattere speciale ($ % @ # § =)
- . non corrispondere a parole facilmente riconducibili all'utente, quali cognome e nome propri o di parenti, date di nascita o di altri eventi noti (es. del matrimonio), il numero di cellulare ecc.
- . essere composta da più parole, eventualmente sostituendo alcune le lettere con la cifra numerica somigliante, es "5" per "S", "8" per "B", "1" per "I" ecc.
- . essere modificata al primo utilizzo;
- essere modificata almeno ogni 6 mesi (3 mesi per chi tratta dati relativi a condanne penali e reati e i dati sanitari e genetici).

E' inoltre una precisa responsabilità dei dipendenti che trattano dati personali (incaricati e responsabili del trattamento):

- mantenerla segreta ed in particolare non condividerla con altre persone e non trascriverla in luoghi prossimi alla postazione di lavoro.

Il sistema operativo presente sulla postazione di lavoro potrà introdurre regole più restrittive, ad esempio il divieto di riuso di password già utilizzate.

Gestione dell'accesso ai dati personali

Sulla base delle analisi effettuate per individuare i dati con particolari requisiti di riservatezza sarà implementata la compartimentazione dei dati in cartelle il cui accesso sarà regolato da specifici criteri di accesso (ACL).
I Responsabili del Trattamento comunicano al Servizio Informatico Associato le specifiche autorizzazione degli incaricati rispetto ai trattamenti di propria competenza.

I Responsabili procederanno altresì all'individuazione degli ambiti di riservatezza che richiederanno la crittografia dei dati.