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 pulita

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.