ESTAR
Ente di supporto tecnico-amministrativo regionale

Allegato ai contratti di assistenza e manutenzione software
Specifiche in merito alla privacy

La particolare delicatezza dei dati trattati per mezzo dei sistemi informatici, sia in ambito sanitario che in ambito ESTAR impone un alto livello di attenzione per garantire il pieno rispetto degli obblighi imposti dalla normativa in vigore in tema di privacy (D.lgs 196/2013 e successive modificazioni; provvedimenti e direttive del Garante della Protezione dei dati personali).
Le nuove procedure informatiche, e i successivi interventi di manutenzione correttiva ed evolutiva, dovranno risultare adeguate alle norme vigenti e alle direttive del Garante in materia di sicurezza e privacy, implementate secondo i paradigmi della "privacy by design", con particolare riferimento ai principi fondanti:

1) Proattivo e non reattivo: prevenire e non correggere
2) Privacy come impostazione di default (privacy by default)
3) Privacy incorporata nella progettazione
4) Piena protezione del ciclo vitale del software/sistema informatico

Relativamente agli applicativi esistenti, il fornitore deve produrre apposita dichiarazione di conformità degli stessi. In particolare in caso di fornitura/manutenzione software deve essere compilato almeno il modulo "Estar – Compliance Privacy Software".
Ove le procedure non risultassero adeguate, è richiesta la stesura di un piano che evidenzi le parti/funzionalità che presentano criticità e la realizzazione di tutti gli interventi necessari per il loro adeguamento, da effettuarsi obbligatoriamente entro sei mesi dalla rilevazione e/o della disposizione normativa sopravvenuta in costanza di rapporto, salvi tempi più cogenti imposti dalla norma o da eventuali prescrizioni del Garante. Si evidenzia che tali interventi rientrano a tutti gli effetti nella manutenzione normativa e dovranno essere assoggettati a specifico collaudo.
L'informativa e il piano di adeguamento saranno oggetto di comunicazione verso le Aziende Sanitarie interessate.
L'attività di manutenzione e assistenza comporta la possibilità di accesso ai dati trattati con i programmi/sistemi informatici oggetto del rapporto (es.: conversione o ripristino data base, recupero dati, teleassistenza, etc.). Le Aziende Sanitarie, nella loro qualità di Titolare del Trattamento di dati personali ai sensi del D. Lgs. n. 196/2003, dovranno procedere a nominare il fornitore Responsabile Esterno del trattamento dei dati. Il documento di nomina potrà contenere analitica specificazione degli obblighi derivanti dalla funzione di Responsabile Esterno del trattamento che, in quanto dettati da obiettivi di rispetto della normativa e della tutela del patrimonio informativo dell'azienda, sono da considerarsi clausole integrative del presente contratto inerenti l'adeguamento normativo e quindi da effettuarsi senza oneri aggiuntivi.
Il Fornitore sarà tenuto a:

- trattare i dati personali nel pieno rispetto della normativa sulla protezione dei dati personali in vigore, operando nell'assoluto rispetto della riservatezza di qualsiasi dato o informazione ovvero di quant'altro venga a conoscenza per effetto dei servizi svolti;
- individuare nominativamente e formare gli Incaricati al Trattamento, comunicandoli al Titolare dei dati ogni qualvolta ne faccia richiesta;
- dare piena applicazione, per quanto di competenza, alle misure di sicurezza di cui agli artt. 31-32-33-34-35-36 del D. Lgs n. 196/2003 ed al disciplinare tecnico Allegato B allo stesso D. Lgs 30/06/2003 n. 196 e sue modifiche ed integrazioni.

Le attività oggetto di fornitura del presente contratto, prevedono specificamente l'opera di figure professionali dotati di capacità ed esperienza nella gestione e nella manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi e le reti di comunicazione.

In relazione al provvedimento del Garante per la protezione dei dati personali datato 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008)", il fornitore è tenuto a individuare gli amministratori di sistema, dettagliando analiticamente l'ambito di operatività degli stessi, in base al profilo di autorizzazione assegnato.
Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante. L'elenco deve essere fornito alla Azienda Sanitaria e/o ad ESTAR ogni qualvolta ne faccia richiesta.
Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, al fine di consentire al Titolare di rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, il fornitore è tenuto a inviare l'elenco degli amministratori e ad inviare gli aggiornamenti in caso di variazione dei nominativi e/o delle competenze assegnate.
Poiché l'attività si esplica mediante interventi ripetuti nel tempo, e modalità di accesso ai dati (es. da remoto; su backup; asportando dischi) che definiscono una reale autonomia operativa sui dati e sui sistemi, è categoricamente esclusa la definizione di "intervento occasionale", per cui tutti gli operatori interessati devono rientrare nella definizione di amministratore di sistema.
Il fornitore, come attività normale di manutenzione, fornisce il supporto sistemistico per i server fisici e virtuali dove sono installati i software del Fornitore.