ALLEGATO IV

Elenco dei sub-responsabili del trattamento

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento :

***Sub*-Responsabile del trattamento** **(Nome, ragione sociale, sede legale)**	**Descrizione del trattamento** (compresa la delimitazione delle responsabilità qualora siano autorizzati più sub- Responsabili)	**Attività svolte per conto del primo Responsabile**	**Dati di contatto del referente (**nome, indirizzo, persona di contatto)

ALLEGATO V
Disciplina dei servizi di Amministratore di Sistema

NOTA ESPLICATIVA: da utilizzare quando le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema

Le persone fisiche designate AdS sono individuate in base ai criteri forniti nel provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009, che considera come tali le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Il Responsabile del trattamento tiene un registro aggiornato di tutti gli Amministratori di Sistema (AdS) nonché di quegli Amministratori di Sistema la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (AdS/L) nominati al momento della sottoscrizione del presente contratto. Ciò anche al fine di consentire al Titolare di rendere nota o conoscibile l'identità degli AdS/L in relazione ai diversi servizi informatici cui questi sono preposti.
Il Responsabile tiene costantemente aggiornato il registro nella forma di seguito indicata

e informa per iscritto il Titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di Amministratori di Sistema.

[in alternativa]

e in caso di accertamenti da parte del Garante o su richiesta del Titolare del trattamento, gli fornisce prontamente e comunque entro 24 ore il medesimo allegato

Col. 1 Cognome e Nome della persona fisica designata AdS	**Col. 2** Società e Organizzazione di appartenenza	**Col. 3** Ubicazione di lavoro dell'Ads	**Col. 4** Funzioni attribuite all'AdS: ambito di operatività per settori o per aree operative (*job description*)	**Col. 5** Banca dati gestita e trattamenti consentiti	**Col. 6** La persona in questione tratta informazioni di carattere personale dei lavoratori (AdS/L)?	
					SI	NO

Legenda:
Colonna 1: Cognome e Nome: cognome e nome della persona fisica che è stata designata, per iscritto, Amministratore di Sistema
Colonna 2: *Organizzazione di appartenenza*: indica la ragione sociale della Società di appartenenza dell'AdS e gli estremi identificativi dell'unità organizzativa nella quale l'AdS opera.
Colonna 3: Ubicazione: indica l'ubicazione di lavoro nella quale l'AdS svolge normalmente la sua attività
Colonna 4: Funzioni attribuite: descrive l'elenco dei servizi informatici assegnati alla persona, l'ambito di operatività per settori o per aree operativa. Vale a dire la *job description* dell'AdS.
Colonna 5: *Banca dati gestita e trattamenti consentiti:* indica le banche dati a cui l'AdS è autorizzato ad accedere e il tipo di operazioni consentite sui dati ivi contenuti. Vale adire il "profilo di autorizzazione" dell'AdS.
Colonna 6: Trattamento di informazioni dei lavoratori (AdS/L): la colonna "SI" indica quegli AdS la cui attività, in relazione ai diversi servizi informatici cui sono preposti, riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (per brevità: "AdS/L"). Il dato viene fornito in adempimento a quanto prescritto dal Provvedimento del Garante che pone a carico dei Titolari del trattamento l'obbligo di rendere nota, nell'ambito della propria organizzazione, l'identità degli AdS/L al fine di richiamare l'attenzione sulla rilevanza e la criticità insite nello svolgimento della loro mansione.

Il Responsabile del trattamento, si impegna più specificamente a:

1) individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
2) assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:
    a. divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;
    b. utilizzo di utenze amministrative anonime, quali "root" di Unix o "Administrator" di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
    c. disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;
3) associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:
    a. utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;
    b. cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password aging).
    c. le password devono differire dalle ultime 5 utilizzate (password history);
    d. conservare le password in modo da garantirne disponibilità e riservatezza;
    e. registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli Amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;
    f. assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;
4) assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
5) assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a

quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;

6) mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa;
7) adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la Società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
8) impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'Amministratore di accedere con una utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;
9) utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;
10) comunicare al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, alla Regione gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:
    a. il nome e cognome;
    b. la user id assegnata agli Amministratori;
    c. il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
    d. i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;
11) eseguire, con cadenza almeno annuale, le attività di verifica dell'operato degli Amministratori e consentire comunque alla Regione Lazio, ove ne faccia richiesta, di eseguire in proprio dette verifiche;
12) nei limiti dell'incarico affidato, mettere a disposizione del Titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;
13) durante l'esecuzione dei Contratti, nell'eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica e/o organizzativa), la Società. si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.