

Egr. Sig.

Rossi Mario

Oggetto: NOMINA DELL'AMMINISTRATORE DI SISTEMA

Ai sensi del "provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, il sottoscritto Rossi Mario in qualità di legale rappresentante di **consorzio infotel**, avendo provveduto ad una preventiva valutazione della capacità, affidabilità nonché dell'esperienza del soggetto di seguito indicato

nomina

il/la Sig./Sig.ra Rossi Mario quale Amministratore di sistema e preposto alla custodia delle parole chiave e/o dei codici identificativi personali ai fini dell'attività di trattamento dei dati personali svolta nella sede via Strauss 45

Il/la Sig./Sig.ra Rossi Mario **accetta la nomina** e si impegna ad operare, seguendo le direttive della **consorzio infotel** impartite (dal Responsabile/dal legale rappresentante), in relazione alle operazioni di trattamento dei dati e a tutto quanto connesso con tale attività come di seguito specificato, al fine di evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta, in armonia con gli obblighi che gli derivano previsti dal D. Lgs. 196/03 e in particolare dall'allegato B alla norma medesima. Le attività e banche dati/sistemi informativi di sua competenza sono riportate in dettaglio in **ALL. 1**.

In particolare, alla luce di quanto previsto nella norma surrichiamata, l'amministratore di sistema ha i seguenti **compiti**:

- a. Il nominato verificherà il corretto funzionamento della rete locale, installerà i programmi indicati dal Titolare, suggerirà la risoluzione dei problemi relativi alla connessione e al regolare funzionamento del sistema, organizzerà e gestirà la posta elettronica e il collegamento a Internet e il sito web, proporrà la pianificazione delle espansioni future della rete (anche di una eventuale rete intranet tra le diverse sedi della società), installerà nuove stazioni di lavoro e di periferiche di rete garantendone il corretto funzionamento, organizzerà e verificherà il backup del sistema e l'archiviazione di file importanti, controllerà le prestazioni del sistema, installerà gli aggiornamenti hardware e software, identificherà i fabbisogni formativi dei dipendenti e collaboratori di **consorzio infotel** e provvederà altresì ad effettuare prove periodiche di ripristino dei dati.
- b. Il nominato svolgerà il predetto incarico attenendosi alle istruzioni ricevute (dal Responsabile/Legale rappresentante) ed ai criteri previsti dalla normativa vigente sulla tutela dei dati personali e sulle misure di sicurezza relative, anche con riferimento ai regolamenti ed alle modalità tecniche adottate da questa Società.
- c. Il nominato Amministratore di sistema avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate e secondo aggiornati criteri tecnici di sicurezza, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dei dati personali, attenendosi a quanto previsto nell'allegato B del D. Lgs. 196/03 (a

- titolo esemplificativo e non esaustivo: password da al meno 8 caratteri possibilmente alfanumerica, sostituzione della stessa ogni tre mesi).
- d. Il nominato amministratore dovrà proporre, al titolare e/o al responsabile del trattamento, l'adozione di programmi antivirus, firewall ed altri strumenti, sia software che hardware, che garantiscano, anche in relazione alle conoscenze acquisite in base al progresso tecnico, la sicurezza nel trattamento dei dati personali secondo i criteri generali stabiliti dall'allegato B del D. Lgs. 196/03 e nelle altre norme a queste connesse in materia di sicurezza, verificandone l'efficacia almeno una volta ogni sei mesi.
 - e. Il nominato amministratore di sistema avrà il compito di controllare periodicamente l'efficienza dei sistemi tecnici, comunque adottati, per verificarne la validità, anche secondo consolidati criteri tecnici di valutazione. Di detti controlli l'amministratore dovrà redigere un apposito verbale che dovrà contenere l'indicazione di coloro che vi hanno partecipato, le modalità di controllo effettuato ed altresì gli strumenti, di qualsiasi natura, utilizzati per provvedervi, i risultati ottenuti ed eventualmente gli ulteriori accorgimenti da adottare onde implementare la sicurezza del trattamento.
 - f. Il nominato amministratore dovrà altresì vigilare - secondo le prassi istituite ed in accordo con gli altri collaboratori del titolare (responsabili del trattamento), che gli individuati incaricati al trattamento dei dati si attengano alle procedure di volta in volta indicate specificamente, sia oralmente che per iscritto, anche in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento secondo il dettato dell'allegato B del D. Lgs. 196/03.
 - g. Il nominato amministratore di sistema dovrà almeno annualmente redigere e/o aggiornare, anche in collaborazione con il Titolare e con il responsabile del trattamento, la parte del documento programmatico relativa a tutta l'attività logica di trattamento dei dati che si svolge mediante reti di elaboratori o terminali sia accessibili che non accessibili al pubblico attraverso reti di telecomunicazioni ed assistere il titolare e/o il responsabile del trattamento nella individuazione degli altri criteri di sicurezza da adottare sia organizzativi che fisici.
 - h. Il nominato amministratore dovrà anche individuare, unitamente al titolare e/o al responsabile del trattamento dei dati, le modalità e le procedure di reimpiego dei supporti di memorizzazione logica ai sensi dell'allegato B del D. Lgs. 196/03 e, se del caso, individuare gli strumenti e le procedure adeguate per procedere alla distruzione e smaltimento dei supporti di memorizzazione che non possono essere riutilizzati. L'amministratore di sistema unitamente al titolare e/o al responsabile del trattamento redigerà in ogni caso un'apposita istruzione operativa in cui siano indicati i supporti che possono essere reimpiegati e/o distrutti, le modalità tecniche adottate sia nel caso di reimpiego che di distruzione e le persone alle quali dette incombenze siano affidate.
 - i. Il nominato amministratore dovrà collaborare con il titolare e/o il responsabile del trattamento dei dati, alla stesura di un disciplinare relativo all'uso delle strumentazioni elettroniche aziendali e attenersi alle regole ivi indicate.
 - j. Il nominato amministratore di sistema intratterrà stretti rapporti di assistenza tecnica continuativa, informazione e comunicazione con il titolare ed il responsabile del trattamento.
 - k. A seguito delle direttive ricevute (Rossi Mario) il nominato sovrintenderà all'assegnazione ed alla custodia delle parole chiave e/o dei codici identificativi personali e - qualora sia opportuno ai fini della sicurezza - alla loro sostituzione nonché alla sospensione dell'abilitazione all'accesso agli strumenti elettronici o automatizzati destinati al trattamento.

- l. Il nominato sarà responsabile del codice identificativo personale assegnatogli come amministratore di sistema e vigilerà ai fini di evitare e prevenire intrusioni ex art. 615 quinquies c.p. - anche adottando e/o facendo adottare idonei programmi antivirus - e verificando l'efficienza dei sistemi di protezione ed accesso mediante eventuali badges o con gli altri sistemi automatici di controllo degli accessi in aree c.d. "militarizzate" e ciò anche in collaborazione con l'addetto alla sicurezza fisica dei locali ove si svolge il trattamento.
- m. Il nominato avrà, altresì, il compito di vigilare - secondo le prassi istituite ed in accordo con il titolare e/o con il responsabile del trattamento, che gli individuati incaricati al trattamento dei dati si attengano alle procedure di volta in volta indicate specificamente, sia oralmente che per iscritto, anche in ordine alla custodia e segretezza della parola chiave e/o dei codici identificativi loro assegnata ed altresì in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento secondo il dettato dell'allegato B del D. Lgs. 196/03.

Si informa altresì, l'Amministratore di sistema che:

1. Gli estremi identificativi dell'amministratore di sistema e le funzioni che gli sono state attribuite, saranno riportati nel documento programmatico sulla sicurezza;
2. consorzio infotel, in qualità di titolare, provvederà a rendere nota o conoscibile l'identità dell'amministratore di sistema nell'ambito della propria organizzazione;
3. L'operato dell'amministratore di sistema sarà oggetto, con cadenza annuale entro il 31 marzo, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. Le ricordiamo, che il provvedimento del Garante già citato, obbliga l'azienda alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti che si allegano alla presente;
4. consorzio infotel adotta sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema. Le registrazioni (access log) avranno le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un periodo di 7 mesi.

Il Titolare **consorzio infotel** sottoscritto Rossi Mario dichiara di accettare l'incarico sopra conferito.

L'Amministratore di Sistema _____
Data, _____

ALLEGATO 1

BANCA DATI/SISTEMA INFORMATIVO	ATTIVITA'
<p>Rossi Mario</p>	<p>Attribuire a ciascun incaricato del trattamento, un codice identificativo personale per l'utilizzazione dell'elaboratore (si deduce dalle regole 1-2 allegato B).</p> <p>Ad ogni incaricato possono essere assegnate una o più credenziali per l'autenticazione (regola 3 allegato B).</p> <p>Non assegnare il codice per l'identificazione, ad altri incaricati, neppure in tempi diversi. Quindi non rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password (regola 6 allegato B)</p> <p>Disattivare le credenziali di autenticazione non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (regola 7 allegato B)</p> <p>Disattivare le credenziali in caso di perdita della qualità (regola 8 allegato B)</p> <p>Disporre ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili (regola 10 allegato B)</p> <p>Provvedere affinché gli elaboratori del sistema informativo siano protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del Codice Penale, mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno</p>

	<p>semestrale (regola 16 allegato B).</p> <p>Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e' almeno semestrale (regola 17 allegato B).</p> <p>Assistere il responsabile del trattamento, in particolare, per quanto concerne l'analisi dei rischi presso la propria Struttura e per le informazioni che il responsabile è tenuto ad inviare al titolare per la stesura annuale del Documento Programmatico di Sicurezza (DPS) (misura idonea).</p> <p>Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso deve essere utilizzato un sistema di autorizzazione (regola 12 allegato B).</p> <p>I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento (regola 13 allegato B).</p> <p>Periodicamente, e comunque almeno annualmente, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (regola 14 allegato B).</p> <p>Assegnare idonei strumenti elettronici a chi tratta dati sensibili o giudiziari per proteggerli contro l'accesso abusivo, di cui all'art.615-ter del codice penale (regola 20 allegato B).</p> <p>Devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati sensibili o giudiziari in caso di danneggiamento</p>
--	---

	degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (regola 23 allegato B).
--	---

ESEMPIO DI STAMPA CONSORZIO INFOTEL