ÆQUA ROMA

Istruzioni Operative per gli Incaricati del Trattamento dei dati

ÆQUA ROMA

INDICE

1. SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di fornire agli **Incaricati** del trattamento di Æqua Roma S.p.A. le necessarie istruzioni volte a garantire che i trattamenti di dati personali siano effettuati nel rispetto delle **Misure Minime di Sicurezza**, previste dall'allegato B del Decreto Legislativo n. 196 del 30 Giugno 2003 (**Codice in materia di protezione dei dati personali**, di seguito Codice).

Il documento è organizzato nelle seguenti sezioni:

- **Documenti di riferimento:** in questo paragrafo è riportato l'elenco dei documenti (quadro normativo vigente in materia di protezione dei dati, procedure aziendali, etc.) a cui si è fatto riferimento per la stesura delle presenti istruzioni;
- **Introduzione:** fornisce una breve panoramica sulle definizioni chiave riportate nel Codice, focalizzandosi sul ruolo dell'incaricato del trattamento all'interno dell'Azienda;
- **Principi Generali:** sono riportate le disposizioni generali che gli incaricati devono rispettare nel trattamento di dati e le misure minime di sicurezza da adottare in caso di trattamento effettuato con o senza **strumenti elettronici**;
- **Conclusioni.**
- **Glossario**: è riportata una sintetica definizione dei termini più ricorrenti nell'ambito della **privacy,** alcuni dei quali sono presenti in questo documento in grassetto.

2. DOCUMENTI DI RIFERIMENTO

- ✓ Codice in materia di protezione dei dati personali (D.lgs. 196/2003);
- ✓ Documento Programmatico sulla Sicurezza approvato dal CDA il….;
- ✓ Standard Operativo Gestione Risorse tecnologiche aziendale approvato dal Presidente il 22/04/2015.

3. INTRODUZIONE

L'articolo 30, comma 1 del D.lgs. 196/2003 prevede che le operazioni di trattamento di dati personali possono essere svolte solo da incaricati, che operano sotto la diretta autorità del Titolare o del Responsabile.

Il ***Titolare del Trattamento*** è Æqua Roma S.P.A, secondo quanto previsto dall'art. 28 del Codice, cui competono le decisioni circa le finalità e le modalità di trattamento di dati personali, ivi compresa la sicurezza dei dati.

Il ***Responsabile del Trattamento*** è la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro Ente, associazione od organismo che il Titolare ha designato per procedere al trattamento dei dati personali.

Il Titolare del trattamento, in relazione all'attività svolta, può individuare, nominare ed incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili di specifici trattamenti con il compito di individuare, nominare ed incaricare per iscritto gli Incaricati del trattamento dei dati personali.

I Responsabili del Trattamento possono essere nominati tra soggetti che per esperienza, capacità e affidabilità diano idonea garanzia del rispetto delle disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza.
In Æqua Roma sono:

- Chiaromonte Silvia per la struttura aziendale AREA RISORSE UMANE E TECNOLOGICHE;
- De Iorio Diego per la struttura aziendale DIREZIONE FISCALITA' IMMOBILIARE;
- Della Valle Gian Luca per la struttura aziendale AREA LOGISTICA ED APPROVVIGIONAMENTI;
- Giattino Gianluca per la struttura aziendale DIREZIONE FISCALITA' ATTIVITA' PRODUTTIVE E RICETTIVE.

Infine, vi sono gli ***Incaricati*** del trattamento che sono le persone fisiche che compiono le operazioni del trattamento dei dati personali, attenendosi alle istruzioni impartite dal Titolare e/o Responsabile.
Tali operazioni possono riguardare la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, la **diffusione**, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il **blocco**, la **comunicazione**, la cancellazione e la distruzione dei dati, anche se non registrati in una banca di dati.

Tali trattamenti potranno essere effettuati con o senza l'ausilio di strumenti elettronici, su **banche dati** informatiche e cartacee e potranno riguardare le seguenti tipologie di dati personali:

- *Dati comuni:* sono le informazioni riferite a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- *Dati sensibili:* sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- *Dati Giudiziari:* sono i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

4. PRINCIPI GENERALI

In ottemperanza alle disposizioni del Codice ed in relazione alle attività svolte nell'ambito della struttura aziendale di appartenenza, l'incaricato, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Responsabile del trattamento.

I dati personali devono essere:

a) Trattati in modo lecito e secondo correttezza e in osservanza dei criteri di riservatezza nei confronti dell'**interessato**;

b) Raccolti per un periodo di tempo non superiore a quello necessario agli scopi, espliciti e legittimi, per i quali vengono trattati;
c) Adeguati, pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
d) Esatti e, se necessario, aggiornati;
e) Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) Trattati nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure minime di sicurezza (di cui agli artt. 33 – 36 ed allegato B del citato Dlgs. 196/03) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. senza l'ausilio di **strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. con strumenti elettronici.

4.1 Trattamenti senza l'ausilio di strumenti elettronici

Lo scopo di questa sezione è quello di illustrare le regole che gli Incaricati devono seguire e rispettare quando trattano Dati Comuni e/o Sensibili e/o Giudiziari in modalità manuale, ovvero mediante l'utilizzo di archivi e documenti cartacei.

Gli Incaricati sono tenuti a custodire diligentemente gli atti e i documenti contenenti dati personali affinché essi siano preservati da danneggiamenti e/o smarrimenti ed a operare in modo da consentire l'accesso esclusivamente:

- all'Interessato a cui tali dati si riferiscono;
- al Responsabile del trattamento di quella tipologia di dato;
- agli altri incaricati a trattare quella tipologia di dato.

A tal fine, per evitare accessi non autorizzati è richiesto che:

1. I documenti contenenti dati personali, siano custoditi in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti, garantendo, quindi, la riservatezza e l'integrità dei dati in essi contenuti (es. armadi o cassetti chiusi a chiave);
2. Le chiavi siano riposte in un luogo sicuro e non lasciate nelle serrature stesse;
3. I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, siano in essi riposti a fine giornata e trasferiti presso gli archivi centrali quando non più operativamente necessari;
4. I documenti contenenti dati personali non rimangano incustoditi su scrivanie o tavoli di lavoro, soprattutto se accessibili al pubblico;

5. I documenti contenenti dati personali non siano condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento);
6. Qualora sia necessario distruggere i documenti contenti dati personali, questi vengano distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, siano sminuzzati in modo da non essere più ricomponibili;
7. L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari avvenga in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave;
8. La conservazione dei dati che rivelano lo stato di salute e la vita sessuale sia effettuata separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

La riproduzione di documenti contenenti dati personali sensibili su supporti non informatici (ad esempio fotocopie) è vietata se non espressamente autorizzata preventivamente e specificatamente dal Responsabile competente o se richiesta dall'interessato. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

4.2 Trattamenti con l'ausilio di strumenti elettronici

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Il processo di **autenticazione informatica**, tramite il quale un sistema elettronico verifica l'identità dichiarata dall'utente, presuppone l'assegnazione preventiva di credenziali di autenticazione che consistono in un codice per l'identificazione dell'incaricato (username) associato a una **parola chiave** riservata (password) conosciuta solamente dal medesimo.

L'accesso alle applicazioni ed alle banche dati di Æqua Roma S.p.a., con cui sono effettuati i trattamenti di dati personali, deve essere, pertanto, consentito ai soli incaricati autorizzati dal Responsabile del trattamento dati di riferimento e, quindi, dotati di credenziali di accesso.
Per motivi tecnici e per semplicità, l'accesso alle Banche Dati ed agli Applicativi aziendali è consentito con la stessa password di accesso al sistema.

La competenza alla richiesta, revoca, modifica del profilo delle autorizzazioni è del Responsabile della U.O. di appartenenza del lavoratore incaricato.

Le password sono assegnate e comunicate in forma riservata agli incaricati dall'Amministratore di Sistema preposto alla gestione delle credenziali. Il lavoratore deve provvedere, al primo utilizzo, alla sostituzione della password provvisoria assegnata con una conosciuta solo dal medesimo**,** attenendosi alle raccomandazioni fornite nel paragrafo successivo.

Il mancato uso delle credenziali per almeno 6 mesi continuativi determina la loro disattivazione.
Per riattivare le credenziali, l'incaricato dovrà rivolgersi all'U. O. Sistemi Informativi ed Infrastrutture Reti Informatiche che provvederà, previa identificazione personale, a fornire una password provvisoria che dovrà essere sostituita da una definitiva.

L'incaricato è tenuto, inoltre, ad assicurare la segretezza della sola password e non della username. Il presupposto essenziale per garantire la sicurezza dei dati è, infatti, che la parola chiave rimanga riservata.

4.2.1 Cosa fare per mantenere segreta la parola chiave

Per proteggere il sistema da accessi non autorizzati, ogni incaricato è tenuto a mantenere segreta la password, mediante l'osservazione delle seguenti istruzioni:

- Non condividere o comunicare a nessuno le proprie password. Ogni incaricato ne è direttamente responsabile, pertanto, qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla;
- Non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;
- Non usare come password parole che possano essere facilmente riconducibili all'identità dell'utente;
- Modificare la password assegnata all'incaricato al primo utilizzo e, successivamente, almeno ogni mese;
- Non sostituire la password con una frequenza superiore alle 2 volte al giorno;
- Comunicare prontamente la perdita, la dimenticanza o la diffusione di una password personale al Responsabile del Trattamento, al Responsabile di riferimento e al Responsabile U.O. Sistemi Informativi e Infrastrutture;
- Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera;
- In presenza di utenti esterni fare attendere questi ultimi in luoghi in cui non siano presenti informazioni riservate o dati personali;
- Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Non installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione del Responsabile del trattamento. Non modificare le configurazioni hardware e software senza l'autorizzazione del Responsabile del trattamento;
- Accertarsi che sul proprio computer sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;
- Utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- Non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

4.2.2 Cosa fare per creare una password idonea

E' di fondamentale importanza proteggere i propri dati utilizzando password complesse, mediante l'osservazione di semplici regole:

1. La password deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
2. Utilizzare caratteri alfabetici (A-Z), numerici (0-9) e caratteri speciali (@, #, $, %);
3. Utilizzare almeno un carattere appartenente a ciascuno degli insiemi sopra enunciati;
4. Nei casi in cui non risulti possibile l'utilizzo dei caratteri speciali, utilizzare caratteri numerici ed alfabetici ripartibili in numero compreso tra un minimo di 3 ed un massimo di 5, ferma restando la lunghezza minima complessiva fissata in 8 caratteri;
5. Non usare più di 3 caratteri uguali consecutivi;
6. Non usare caratteri di spaziatura;
7. Non usare per la password alcuna parte della username;
8. Le password non dovrebbero contenere:
    - ✓ nomi propri di persona;
    - ✓ sigle di funzioni organizzative o progetti interni all'azienda;
    - ✓ nomi di giorni della settimana, mesi dell'anno o stagioni;
    - ✓ nomi di riferimenti geografici;
    - ✓ nomi di personaggi della politica, sport, cinema e fumetti.
    - ✓ riferimenti al corrispettivo identificativo utente;
    - ✓ il nome o cognome dell'incaricato;
    - ✓ la matricola dell'incaricato;
    - ✓ la data di nascita dell'incaricato;
    - ✓ esclusivamente date in qualsiasi formato e con qualsiasi separatore di uso comune.
9. Ogni nuova password dovrebbe differire dalla precedente perlomeno in 4 caratteri.

4.2.3 Cosa fare per custodire diligentemente gli strumenti elettronici aziendali

Non è consentito che due o più Incaricati al trattamento accedano al sistema, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente e la medesima password.

Nel caso in cui un incaricato abbia necessità di assentarsi temporaneamente dalla postazione di lavoro, deve assicurarsi che nessuno possa accedere ai dati personali del sistema durante la sua assenza, mediante uno dei seguenti accorgimenti:

- Attivare il blocco del sistema ponendolo in stato di *lock.* Tale operazione può essere effettuata premendo in sequenza i tasti ctrl+alt+canc e quindi cliccando sul pulsante "blocca computer";
- Chiudere a chiave la porta quando si esce dal proprio ufficio quando vi è necessità di assentarsi in modo prolungato dalla propria postazione di lavoro.
- Spegnere il sistema.

5. CONCLUSIONI

Æqua Roma S.p.a., tramite verifiche periodiche, direttamente o con l'ausilio di altre società, effettuerà i controlli che riterrà opportuni per vigilare sulla puntuale osservanza delle disposizioni della normativa vigente e delle presenti istruzioni operative.

Si rammenta che la violazione delle misure minime di sicurezza e della normativa in tema di corretto trattamento dei dati comporta l'applicazione di sanzioni amministrative e penali, anche nel caso in cui non ci siano parti lese.

GLOSSARIO

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Banca Dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Codice in materia di protezione dei dati personali (D.Lgs. 196/2003)

Testo unico in materia di protezione di dati personali, entrato in vigore dal 1 Gennaio 2004 che sostituisce la precedente Legge 675/96 e integra in numerosi decreti e provvedimenti emanati dal 1997 al 2003.

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Consenso

La libera manifestazione della volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, sul quale è stato preventivamente informato da chi gestisce i dati (v.d. titolare). E' sufficiente che il consenso sia documentato in forma scritta (ossia, annotato, trascritto, riportato dal Titolare o dal Responsabile o da un Incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati sensibili; in questo caso occorre il consenso esplicito rilasciato per iscritto dall'interessato (ad es. con la sua sottoscrizione).

Credenziali di autenticazione

I dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Dato Anonimo

Dati che in origine, o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile (lettera n, comma 1, art. 4).

Dato personale pubblico

Dato personale di dominio pubblico (es. rubriche telefoniche pubbliche).

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Garante

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla legge sulla privacy (legge n. 675 del 31 dicembre 1996). L'istituzione di analoghe autorità prevista in tutti gli altri Paesi membri dell'Unione Europea (direttiva comunitaria 95/46/CE). Il Garante ha il compito di assicurare la tutela dei diritti e delle libertà fondamentali nel trattamento dei dati personali, ed il rispetto della dignità della persona. Il Garante si compone di quattro membri eletti dal Parlamento, ha sede a Roma (piazza di Monte Citorio, 121). Alle sue dipendenze è posto un Ufficio con un organico di cento unità. Esamina segnalazioni dei cittadini e vigila sul rispetto delle norme che tutelano la vita privata. Decide sui ricorsi presentati dai cittadini e può compiere ispezioni.

Informativa

Le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi: su quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e il responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax ecc.).

Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

Misure Minime di Sicurezza

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Privacy

E' un termine inglese che evoca significati a volte mutevoli, accostabile ai concetti di riservatezza, privatezza. Ad esempio, oggi la privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma anche il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione. Il diritto alla privacy e, in particolare, alla protezione dei dati personali costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.