COMUNE DI APRILIA

Provincia di Latina

REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI E PER LA DISCIPLINA DELLE IPOTESI DI *DATA BREACH*

Approvato con deliberazione G.C. n. 182 del 28.10.2019

Capo I - Principi

ARTICOLO 1 – OGGETTO E AMBITO DI APPLICAZIONE

Il presente Regolamento disciplina l'utilizzo della strumentazione informatica da parte del personale dell'Ente al fine di tutelare i beni comunali e di garantire il loro corretto uso, evitando condotte sanzionabili disciplinarmente, da parte dei dipendenti e/o collaboratori a vario titolo dell'Ente, fatte salve le ipotesi di più gravi illeciti, o comunque condotte che, anche inconsapevolmente, possano costituire una minaccia alla sicurezza del sistema informatico comunale e alla riservatezza dei dati personali trattati e quindi esporre l'Ente anche a potenziali responsabilità nei confronti di terzi.

Il presente Regolamento disciplina, altresì, le procedure per l'individuazione, valutazione ed eventuale comunicazione al Garante della privacy di una violazione di dati personali con riferimento alle attività di trattamento effettuate dal Comune di Aprilia (o da suoi Responsabili "esterni" del trattamento) e stabilisce le modalità operative adottate dall'Ente a tal fine, nel rispetto del principio di responsabilizzazione di cui all'art. 5, co. 2 del Regolamento (UE) 2016/679. Tale disciplina si applica agli Utenti che abbiano accesso a dati personali trattati dal Comune.

Per violazione dei dati personali (c.d. data breach) si intende un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare del trattamento dei dati non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del Regolamento (UE) 2016/679. Essa si definisce come la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, divulgazione non autorizzata di dati personali.

Le disposizioni ivi previste hanno carattere organizzativo e mirano a conformare i processi amministrativo-gestionali dell'Ente ai principi di diligenza, informazione e correttezza, anche nell'ambito del rapporto di lavoro: gli eventuali controlli volti a verificare il rispetto del presente Regolamento non hanno finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono effettuati ai sensi e nel rispetto della normativa vigente, in particolare con riferimento al Regolamento (UE) 2016/679, ai vigenti Contratti Collettivi Nazionali di lavoro e ai provvedimenti emanati dal Garante per la Protezione dei dati personali.

Il presente Regolamento si applica a ogni Utente (per tale intendendosi, a titolo esemplificativo, ogni dipendente, collaboratore, consulente, affidatario di servizi che in modo continuativo e non occasionale operi all'interno della struttura comunale utilizzandone beni e servizi informatici) assegnatario di beni e risorse informatiche comunali, ovvero utilizzatore di servizi e risorse informatiche di proprietà del Comune di Aprilia.

ARTICOLO 2 – TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali, da considerarsi di esclusiva proprietà dell'Ente che, in virtù del rapporti instaurati con l'Utente, ne decide l'affidamento.

Il loro utilizzo, pertanto, è consentito dal Comune solo per finalità di svolgimento delle mansioni lavorative assegnate a ciascun Utente in base al rapporto in essere e di adempimento dei correlati obblighi.

Qualsivoglia dato (anche personale) e/o informazione trattati dall'Utente attraverso i beni e le risorse informatiche di proprietà dell'Ente, assegnati all'Utente stesso, sono considerati di natura istituzionale e non personale.

ARTICOLO 3 – RESPONSABILITA' PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo corretto e conforme alle disposizioni del presente Regolamento dei beni e delle risorse informatiche affidatigli dall'Ente, nonché dei dati personali trattati nell'ambito dell'attività lavorativa con il supporto delle predette risorse informatiche. Pertanto, ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, è tenuto a tutelare tali beni e risorse (per quanto di propria competenza) da utilizzi impropri e non autorizzati allo scopo di preservare l'integrità dei medesimi e garantire la riservatezza dei dati e delle informazioni accessibili tramite essi.

E' preciso compito e dovere di ciascun Utente, in rapporto al proprio ruolo e alle mansioni in concreto svolte, operare a tutela della sicurezza informatica del Comune, riferendo al proprio Dirigente, senza ritardo, di possibili violazioni del presente Regolamento di cui sia venuto a conoscenza e/o di eventuali rischi operativi di cui sia in grado di rendersi conto operando con l'ordinaria diligenza richiesta nell'ambito dello specifico rapporto lavorativo con il Comune.

Ogni Utente risponde disciplinarmente, fatte salve le più gravi responsabilità civili, penali e contabili eventualmente accertate, per i danni derivanti da negligenza e imprudenza nell'utilizzo dei beni e risorse informatiche o per il loro improprio utilizzo.

Capo II – Misure organizzative per l'utilizzo degli strumenti informatici

ARTICOLO 4 – AMMINISTRATORI DI SISTEMA

L'Ente conferisce all'Amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche aziendali.

E' compito dell'Amministratore di sistema:

1) gestire gli hardware e i software di tutta la strumentazione informatica di titolarità dell'Ente;

2) gestire la creazione, l'attivazione, la disattivazione degli account di rete e dei relativi privilegi di accesso alle risorse assegnati agli Utenti e tutte le correlate attività amministrative;
3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli Utenti, purché tali attività rientrino nelle normali attività di manutenzione, gestione della sicurezza e protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio, purché tali attività rientrino nelle normali attività di manutenzione, gestione della sicurezza e protezione dei dati;
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli Utenti, purché tali attività rientrino nelle normali attività di manutenzione, gestione della sicurezza e protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto delle previsioni dell'art. 32 del Regolamento (UE) 2016/679;
7) utilizzare le credenziali di accesso di amministratore di sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso: tale attività deve essere richiesta espressamente dal Dirigente del Settore competente al trattamento dei dati e autorizzata dal Segretario Generale e deve essere limitata al tempo strettamente necessario per il compimento delle attività indifferibili per cui è avvenuta la richiesta.

ARTICOLO 5 – ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli account

Gli account vengono creati dall'Amministratore di sistema e sono personali, ovvero associati univocamente alla persona assegnataria. Ogni Utente è responsabile dell'utilizzo corretto e lecito del proprio account.

L'account generato e assegnato all'Utente consente l'identificazione dell'utilizzatore e disciplina l'accesso alle specifiche risorse informatiche aziendali, per ciascuna postazione lavorativa.

L'accesso da parte dell'Utente al proprio account avviene tramite l'utilizzo di "credenziali di autenticazione" (User id e password), comunicate dall'Amministratore di sistema con modalità che ne garantiscano la segretezza (ad es., busta chiusa e sigillata).

Le credenziali di autenticazione costituiscono dati da mantenere strettamente riservati, non è consentito comunicarne gli estremi a terzi, neppure soggetti interni all'Ente, anche se in posizione gerarchicamente superiore o apicale).

Se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate o carpite da qualcuno, o che il proprio account sia utilizzato in modo non autorizzato da parte di soggetti terzi, egli è tenuto a modificare immediatamente la password e a segnalare la violazione con le modalità di cui all'art. 15 del Regolamento.

In caso di assenza improvvisa o prolungata dell'Utente, per esigenze strettamente produttive o per la sicurezza e operatività delle risorse informatiche, l'Ente si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema, come specificato all'art. 4 comma 1 n. 7.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'Amministratore di sistema, l'Utente provvede a modificare, al primo utilizzo, la propria password, procedendo allo stesso modo di volta in volta, secondo le tempistiche stabilite dall'Amministratore di sistema e comunque almeno ogni 3 mesi.

L'Utente, nel definire il valore della password, deve rispettare le regole indicate dall'Amministratore di sistema (per quanto concerne la lunghezza della password, l'utilizzo di caratteri speciali e/o di lettere maiuscole, ecc.), evitando in ogni caso di includere parti del nome, del cognome e/o comunque elementi a lui agevolmente riconducibili, o di utilizzare parole chiave comuni e/o prevedibili.

La password deve essere custodita con la massima cura, al fine di proteggerne la riservatezza, e deve essere utilizzata al solo fine di esercitare i poteri autorizzativi concessi. Annotare la password su un post-it o su altri supporti agevolmente asportabili non è qualificabile come corretta modalità di custodia della stessa e costituisce violazione del presente Regolamento.

Cessazione degli account

In caso di cessazione del rapporto di lavoro, di collaborazione o di consulenza con l'Utente, verrà disposta la chiusura e cancellazione dell'account entro le successive 48 ore.

ARTICOLO 6 – POSTAZIONI DI LAVORO

Per postazione di lavoro (statica e/o mobile) si intende il complesso unitario composto da personal computer (di seguito "PC"), notebook, accessori, supporti *hardware* nonché ogni altro *devic*e consegnato dal Comune e utilizzato dall'Utente per svolgere, a seconda delle mansioni affidate e del rapporto contrattuale in essere, la propria attività lavorativa.

Per assicurare un utilizzo lecito e corretto di tali beni, l'Utente è tenuto ad osservare le seguenti regole:

1. ogni Utente deve utilizzare gli strumenti di lavoro che gli sono stati consegnati in maniera professionale e responsabilmente, ai sensi dell'art. 3;

2. devono essere utilizzati soltanto apparecchi *hardware* e applicativi *software* consegnati e/o preventivamente autorizzati dall'Ente;
3. le postazioni di lavoro non devono essere lasciate incustodite con la sessione di lavoro attiva: quando un Utente si allontana dalla propria postazione di lavoro deve effettuare il log-out della sessione di lavoro, cioè schermo e tastiera devono essere bloccati mediante attivazione dello screensever (con necessità di reintroduzione delle credenziali di autenticazione ai fini dello sblocco);
4. l'utente deve segnalare con la massima tempestività all'Amministratore di sistema eventuali guasti tecnici, problematiche operative o il cattivo funzionamento delle apparecchiature;
5. è fatto divieto di cedere in uso, anche temporaneamente, le attrezzature costituenti la postazione di lavoro assegnata a soggetti terzi.

Gli apparecchi personali dell'Utente, quali computer portatili, smartphone, tablet, fotocamere digitali, non possono essere collegati ai computer o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta dell'Ente (Ufficio di Segreteria Generale) e successiva abilitazione dell'Amministratore di rete.

Capo III – Criteri di utilizzo delle apparecchiature informatiche

ARTICOLO 7 – PERSONAL COMPUTER E COMPUTER PORTATILI

Gli Utenti, per lo svolgimento delle proprie attività lavorative, utilizzano dispositivi di proprietà dell'Ente, rispetto ai quali valgono le seguenti regole:

a) non è consentito modificare la configurazione *hardware* e *software* del proprio PC, se non previa espressa autorizzazione dell'Ente, che viene eseguita dall'Amministrazione di sistema;
b) non è consentito rimuovere o asportare componenti *hardware;*
c) non è consentito installare autonomamente programmi o applicazioni informatici;
d) è onere dell'Utente sospendere ogni attività in caso di minacce di intrusione di virus o altri malfunzionamenti, segnalando prontamente l'accaduto secondo le modalità di cui all'art. 15;
e) ogni Utente è tenuto a spegnere il proprio PC al termine della giornata lavorativa;
f) non è consentito inserire all'interno del PC o del computer portatile dati personali o comunque non attinenti con l'attività lavorativa svolta;
g) l'Utente ha l'obbligo di custodire con diligenza e in luoghi protetti i computer portatili durante gli spostamenti.

In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, gli Utenti sono tenuti a rimuovere tutti i *files* elaborati e a cancellare tutti i dati eventualmente presenti prima di riconsegnare il portatile per la restituzione definitiva o una sua riparazione.

ARTICOLO 8 – SOFTWARE

Quando l'Ente acquisisca le licenze d'uso dei *software* da fornitori esterni l'Utente è soggetto a limitazioni nell'utilizzo di tali programmi, quali risultanti dai termini e condizioni previste nei contratti di licenza, e non ha diritto di riprodurli o di utilizzarli in deroga a quanto stabilito dai contratti in parola.

Non è consentito effettuare il *download* o l'*upload* di programmi e/o applicativi attraverso internet.

Ai sensi di quanto disposto dalle vigenti disposizioni normative in materia di proprietà intellettuale e diritto d'autore, gli utenti coinvolti nella riproduzione, duplicazione e diffusione illegale di programmi informatici sono responsabili sia civilmente che penalmente. Inoltre rispondono nei confronti del Comune sotto il profilo disciplinare.

ARTICOLO 9 – DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi fisici che consentono di copiare o archiviare *files* esternamente rispetto alla memoria del computer o ai server comunali: sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, memory card, dischi rigidi esterni, ecc.

Non è consentito utilizzare supporti rimovibili personali, cioè non consegnati dall'Ente, nell'ambito dell'attività lavorativa propria del rapporto contrattuale in essere con il Comune.

I dispositivi di memoria portatili non devono essere utilizzati come dispositivi di archiviazione e/o stoccaggio di dati perché non protetti né sottoposti a back up.

ARTICOLO 10 – STAMPANTI, SCANNER, FOTOCOPIATRICI

L'utilizzo di tali strumenti deve avvenire esclusivamente per finalità istituzionali e comunque nell'ambito dell'attività riconducibile al rapporto contrattuale in essere con il Comune.

Nel caso di utilizzo di una stampante condivisa tra più Uffici o in caso di stampante posizionata in un luogo accessibile a visitatori esterni occorre utilizzare una particolare attenzione quando si inviano in stampa documenti contenenti dati personali e/o informazioni riservate. In particolare occorre porre in essere tutte le precauzioni per evitare di lasciare incustoditi i documenti stampati e diffondere impropriamente i dati in essi contenuti. Tale regola vale anche in caso di effettuazione di fotocopie di documenti.

Analogamente, quando vengono effettuate scansioni di documenti attraverso uno scanner associato a una "cartella condivisa" sul *server*, una volta completata l'acquisizione dell'immagine, il relativo *file* deve essere salvato nelle apposite cartelle nell'area di lavoro privata dell'Utente e deve essere cancellato dalla "cartella condivisa".

Il passaggio di stato (da digitale ad analogico o da analogico a digitale) dei documenti che contengono dati personali e/o informazioni riservate – che configura un trattamento di dati, sotto forma di elaborazione – deve essere limitato alle ipotesi di stretta necessità lavorativa, in quanto la stampa, la copia e la scansione di documenti, comunque effettuate, danno luogo a forme di duplicazione (se non addirittura moltiplicazione) dei dati personali trattati, mediante replicazione dei supporti documentali in cui essi sono contenuti.

ARTICOLO 11 – STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

L'Ente può mettere a disposizione, a seconda del ruolo ricoperto o della funzione svolta dal singolo Utente, apparecchi di telefonia mobile, nonché dispositivi – quali smartphone e tablet – che consentono di navigare in internet tramite rete di dati e/o del servizio di telefonia tramite rete cellulare.

Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente ai dispositivi sopra indicati. Tali dispositivi devono essere utilizzati soltanto per motivi lavorativi, ancorchè sia consentito l'utilizzo personale sporadico e moderato e comunque salvi casi di necessità e urgenza. Non devono essere comunicati per telefono dati personali e/o informazioni riservate.

Anche su questi apparati l'amministratore di sistema effettua la supervisione e iI controllo ai sensi del precedente articolo 4 del presente Regolamento.

In generale l'utilizzo dei dispositivi deve avvenire nel rispetto delle seguenti regole:

- ogni Utente assegnatario è responsabile dell'uso appropriato e della diligente conservazione del dispositivo;
- ogni dispositivo deve essere dotato di password di autenticazione, codice pin, impronta digitale che ne impedisca l'accesso a soggetti non autorizzati: analogamente le applicazioni installate sul dispositivo che comportino il trattamento di dati personali e/o di informazioni riservate devono essere protette da password / pin / impronta digitale;
- le password / pin devono essere sostituiti ogni 3 mesi;
- ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e del pin: qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a sostituire la password o il pin, dando comunque comunicazione all'Ufficio di Segreteria Generale dell'avvenuta sostituzione e dei motivi;
- in caso di furto, danneggiamento o smarrimento del dispositivo mobile assegnato, l'Utente dovrà darne immediato avviso all'Ufficio Economato e dovrà provvedere a denunciare l'accaduto alle competenti Autorità di polizia;
- non è consentito all'Utente caricare, inserire o salvare all'interno del dispositivo qualunque dato o informazione non attinente con l'attività lavorativa svolta;

- non è consentito all'Utente effettuare con il dispositivo riprese, fotografie, registrazioni di suoni, a meno che non vi sia una espressa richiesta in tal senso da parte dell'Ente;
- l'eventuale installazione di applicazioni, sia gratuite sia a pagamento, su smartphone e tablet deve essere espressamente autorizzata;
- al momento della riconsegna del dispositivo, l'Utente è tenuto a verificare di aver cancellato tutti i dati presenti e di aver disattivato il sistema di geolocalizzazione.

Capo IV – Criteri di utilizzo degli altri strumenti informatici

ARTICOLO 12 – GESTIONE E UTILIZZO DELLA RETE INTERNET

Ogni Utente abilitato dall'Ente alla navigazione su internet per lo svolgimento dell'attività lavorativa oggetto del rapporto contrattuale, dovrà osservate le seguenti norme di comportamento:

- non è consentito navigare su siti internet per finalità private o per scopi diversi da quello di svolgere l'attività lavorativa;
- è vietata ogni forma di registrazione a siti internet e le partecipazioni a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book,* i cui contenuti non siano legati all'attività lavorativa;
- non è consentita la memorizzazione sui supporti informatici consegnati dall'Ente per lo svolgimento dell'attività lavorativa di documenti in formato elettronico di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- è consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi legati all'attività lavorativa e attraverso gli strumenti informatici e i *software* messi a disposizione dall'Ente;
- non è consentito l'utilizzo di social network sul luogo di lavoro o durante l'orario lavorativo, a meno che non sia richiesto dall'Ente in relazione alle attività lavorative da svolgere da parte dell'Utente;
- non è consentito lo scambio e/o la condivisione (ad es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico ecc. protetto da *copyright*;
- non è consentito sfruttare i segni distintivi e ogni altro bene immateriale di proprietà / titolarità dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata prima richiesta o approvata espressamente dall'Ente.

Per assicurare il rispetto di tali regole, l'Ente si riserva, attraverso l'Amministratore di Sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso a determinati contenuti non consentiti e che prevengono operazioni non correlate allo svolgimento delle mansioni lavorative (restrizione nella navigazione, blocco al *download* di *files* e *software*, ecc.).

ARTICOLO 13 – GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA

Ad ogni Utente titolare di un account l'Ente provvede ad assegnare una casella di posta elettronica individuale, associata al dominio dell'Ente, esclusivamente per lo svolgimento dell'attività lavorativa e/o per la gestione dei rapporti tra l'Utente e l'Ente. L'account e-mail associato al dominio dell'Ente costituisce un bene del Comune

Ai fini della denominazione dell'account, può essere utilizzato alternativamente il nome e/o cognome dell'Utente (ad es. mario.rossi@ente.it), oppure la denominazione dell'area funzionale / ufficio in cui opera (ad es. segreteria@ente.it, oppure tesoreria@ente.it).

Attraverso l'indirizzo e-mail, gli Utenti rappresentano pubblicamente l'Ente nella corrispondenza elettronica e nei contatti, per questo motivo, il sistema di posta elettronica deve essere utilizzato in modo da non ledere in alcun modo l'immagine del Comune.

Nell'utilizzare la casella di posta elettronica, gli Utenti devono:

- conservare accuratamente la password, in modo da preservarne la segretezza;
- mantenere la casella in ordine, cancellando e-mail inutili o allegati ingombranti (dopo aver salvato il file) oppure le comunicazioni intercorse con soggetti esterni che siano persone fisiche, ai sensi del Regolamento (UE) 2016/679, in particolare dei principi generali esposti nell'art. 5, e nel rispetto delle procedure e delle tempistiche definite dall'Ente per la conservazione dei dati personali all'interno del Registro per la disciplina del trattamento dei dati personali;
- inviare preferibilmente *files* contenenti dati personali in formato pdf/A;
- verificare l'attendibilità dei *files* allegati ai messaggi di posta elettronica in entrata prima di utilizzarli. In particolare prestare attenzione alla dimensione degli allegati, all'estensione dei file, all'oggetto e all'indirizzo di provenienza dei messaggi e-mail ricevuti: le comunicazioni provenienti da mittenti sconosciuti o riportanti caratteri strani non devono essere aperti, in quanto potenzialmente dannosi per i sistemi informatici;
- collegarsi a link di siti internet contenuti all'interno dei messaggi solo quando vi sia comprovata sicurezza della provenienza dell'e-mail ricevuta.

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura e protocolli di trasmissione, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse, pertanto occorre evitare, per quanto possibile, l'invio tramite e-mail di dati personali e/o informazioni riservate / confidenziali, dovendo piuttosto essere utilizzato il protocollo generale con apposizione della qualifica di "protocollo riservato".

I messaggi di posta elettronica devono contenere un chiaro avvertimento per i destinatari, al fine di informarli della natura non personale del contenuto dei messaggi (che può essere conosciuto dall'Ente).

E’ vietato inviare tramite e-mail credenziali di autenticazione.

In caso di assenze programmate gli Utenti potranno impostare il sistema di gestione della casella di posta elettronica affinché provveda all’invio automatico di messaggi di risposta che informino dell’assenza.

Per le assenze non programmate (ad es. per malattia), qualora l’assenza si protragga per oltre 30 giorni e comunque quando l’Ente necessiti di conoscere il contenuto dei messaggi di posta elettronica, quest’ultimo, avvalendosi dell’Amministratore di sistema e avvertendo l’Utente assente, disporrà la verifica del contenuto dei messaggi per il tramite di un altro soggetto (lavoratore o collaboratore), in veste di “fiduciario” nominato dall’assente o dal superiore gerarchico. Le attività di verifica saranno debitamente verbalizzate e il verbale sarà portato a conoscenza dell’Utente assente al suo rientro.

In caso di cessazione del rapporto di lavoro o di collaborazione, consulenza, fornitura con l’Utente, verrà disposta la chiusura e cancellazione dell’account entro le successive 48 ore. In ogni caso, l’Ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Capo IV – Procedure di gestione e comunicazione delle violazioni di dati personali

ART. 14 – OBBLIGHI DEL TITOLARE

Ai sensi dell’art. 33 del Regolamento (UE) 2016/679, la violazione di dati personali (c.d. *data breach)* deve essere formalmente comunicata al Garante della Privacy, tranne nel caso in cui sia improbabile che la violazione verificatasi in concreto comporti un rischio per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento dei dati ha l’obbligo di identificare l’incidente di sicurezza, quindi comprendere che impatto abbia avuto sulle informazioni e, infine, se tra le informazioni coinvolte dall’incidente vi siano dati personali. Il titolare del trattamento ha l’obbligo di notificare al Garante della Privacy le violazioni di dati personali verificatesi entro 72 ore dalla scoperta della violazione. Quando la notifica avviene oltre il termine delle 72 ore deve essere accompagnata da una relazione che specifichi i motivi del ritardo, pertanto è importante che sia dimostrabile il momento della scoperta dell’incidente.

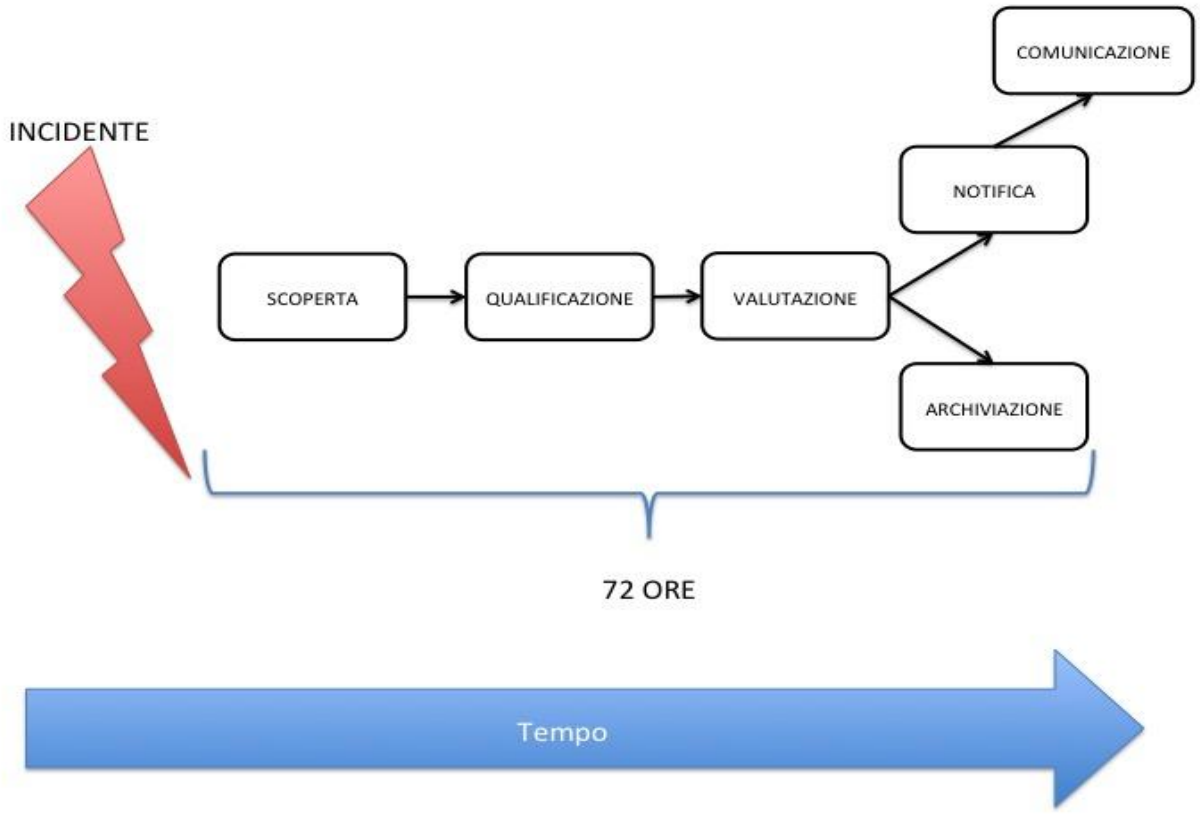
Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l’impatto. La comunicazione del *data breach* all’interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un’accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi dati personali.

Il titolare del trattamento, a prescindere dalla notifica al Garante, documenta tempestivamente

tutte le violazioni dei dati personali e le relative valutazioni compiute, compilando l'apposito "Registro dei *data breach*" istituito e tenuto a cura del Segretario Generale, in qualità di responsabile dell'Ufficio di supporto al Responsabile della protezione dei dati personali (Data Protection Officer) - giusta deliberazione G.C. n. 179/2018 - con il supporto del medesimo Responsabile della protezione dei dati personali.

Il titolare del trattamento deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

Di seguito il flusso procedurale:



ART. 15 – PROCEDURA DI GESTIONE DELL'INCIDENTE DI SICUREZZA

Chiunque all'interno dell'Ente – tra i soggetti qualificati come Utenti dall'art. 1 ultimo comma del presente Regolamento - rilevi, nello svolgimento delle proprie attività lavorative, un incidente che integra o potrebbe integrare una violazione di dati personali, è tenuto a darne immediata comunicazione, con qualunque strumento che appaia efficace tenuto conto del livello di urgenza, (per telefono, di persona, a mezzo e-mail) all'Ufficio di Segreteria Generale, quale ufficio di

supporto al Titolare del trattamento e al Responsabile della protezione dei dati personali, oppure direttamente al Responsabile della protezione dei dati personali. In quest'ultimo caso i recapiti sono pubblicati in Sezione Amministrazione Trasparente.

L'Ufficio di Segreteria Generale informa, ciascuno per gli aspetti di competenza, l'Amministratore di sistema, il Responsabile della protezione dei dati personali e il Responsabile del trattamento dei dati, quest'ultimo individuato a seconda del Settore competente al trattamento dei dati coinvolti nell'incidente di sicurezza.
I soggetti sopra indicati, ognuno nei rispettivi ambiti di competenza, se del caso anche congiuntamente, verificano l'incidente occorso e le sue conseguenze e, ricorrendone i presupposti, provvedono alla qualificazione dello stesso come "violazione di dati personali" stilando apposito verbale. Quindi, entro le 48 ore successive dalla conoscenza dell'evento:

- ne valutano la portata, le eventuali conseguenze, i dati personali interessati e i soggetti potenzialmente coinvolti;
- individuano e adottano le misure di emergenza idonee a contenere gli effetti dannosi e a ripristinare la disponibilità e l'accessibilità dei dati (disaster recovery).

L'Ufficio di Segreteria Generale, entro 60 ore dalla scoperta dell'evento, trasmette un report riepilogativo delle attività sopra indicate al Titolare del trattamento, affinché valuti – con il supporto del Responsabile della protezione dei dati personali – se, in definitiva, ricorrono uno o entrambi i presupposti di cui all'art. 33 del Regolamento per procedere alla notifica al Garante per la protezione dei dati personali ed, eventualmente, anche alla comunicazione agli interessati:
1) la violazione dei dati personali
2) che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

In caso di necessità di notifica, il Titolare del trattamento provvede entro le successive 12 ore, secondo le modalità di cui all'art. 16.

Lo stesso iter procedimentale viene seguito nel caso in cui l'incidente che potrebbe dare luogo a una violazione di dati personali si verifichi e/o venga accertato presso un Responsabile esterno del trattamento: in tal caso le attività di istruttoria preliminare – che confluiscono nel report sopra menzionato – verranno svolte dal Responsabile esterno del trattamento e il relativo verbale verrà comunicato all'Ufficio di Segreteria Generale e al Responsabile della protezione dei dati personali del Comune di Aprilia.

ART. 16 – VALUTAZIONE DEL RISCHIO DELLA VIOLAZIONE DI DATI PERSONALI

A seguito della scoperta il titolare deve essere in grado di valutare la portata dell'incidente in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati, deve cioè essere valutato il rischio della violazione dei dati personali.

Sulla base del verbale di cui all'art. 14 comma 3, redatto dal Responsabile della protezione dei dati, dall'Amministratore di sistema e dal Responsabile del trattamento dei dati, il Titolare del trattamento, con il supporto del Responsabile della protezione dei dati, ai fini della decisione se procedere o meno alla notifica al Garante, provvede a classificare l'evento tra i seguenti casi:

1. distruzione di dati illecita;
2. perdita di dati illecita;
3. modifica di dati illecita;
4. distruzione di dati accidentale;
5. perdita di dati accidentale;
6. modifica di dati accidentale;
7. divulgazione non autorizzata;
8. accesso ai dati personali illecito.

Parallelamente deve essere indagata la caratteristica dei dati violati verificando:

- la natura, il numero e il grado di sensibilità dei dati personali violati;
- la facilità di associare i dati violati ad un persona fisica;
- la gravità delle conseguenze per gli interessati;
- il numero di soggetti esposti al rischio.

In particolare saranno valutate come variabili qualitative del rischio di violazione:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

b) che si tratti di dati relativi a valutazione di aspetti personali - quali il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti - al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di dati personali;

e) che il trattamento riguardi un vasto numero di Interessati;

f) che si verifichi una delle seguenti condizioni a danno di persone fisiche, anche diverse dall'Interessato, a cui si riferiscono i dati:

- discriminazioni;
- furto o usurpazione d'identità;
- perdite finanziarie (furto di denaro);
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- decifratura non autorizzata;
- danno economico o sociale significativo;

- privazione o limitazione di diritti o libertà;
- impedito controllo sui dati personali all'interessato;
- danni fisici, materiali o immateriali alle persone fisiche.

L'esito della valutazione della violazione deve corrispondere ad uno dei seguenti livelli di rischio:
- NULLO
- BASSO
- MEDIO
- ALTO.

ART. 17 – NOTIFICA AL GARANTE DELLA PRIVACY

All'esito dell'attività di valutazione, nei casi in cui sia attestato l'alto rischio di violazioni di dati personali con effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali – secondo i parametri elencati nell'articolo precedente - il Titolare provvede alla notifica al Garante.

La notifica viene effettuata utilizzando, di norma, l'apposito modello predisposto dallo stesso Garante. In ogni caso essa deve contenere almeno le informazioni sinteticamente riportate di seguito (art. 33, par. 3 del Regolamento), desumibili dal primo verbale redatto ai sensi dell'art. 15 comma 3:

- una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:
    - le categorie e il numero approssimativo di persone interessate;
    - le categorie e il volume approssimativo di dati personali interessati;
- il nome e i riferimenti di contatto del responsabile della protezione dei dati o comunque di un referente competente a fornire informazioni;
- una descrizione delle possibili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi;
- in caso di notifica effettuata oltre il termine prescritto di 72 ore, una descrizione dei motivi del ritardo.

La notifica va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it. Secondo le indicazioni dello stesso Garante, l'oggetto del messaggio deve contenere obbligatoriamente la dicitura "notifica violazione dati personali" e opzionalmente la denominazione del titolare del trattamento.

ARTICOLO 18 – SANZIONI

La violazione delle previsioni del presente Regolamento potrà comportare l'applicazione di sanzioni disciplinari integrando una violazione dei doveri del dipendente.

In caso di violazione accertata, l'Ente provvederà a sospendere, bloccare o limitare gli accessi agli account e alle caselle di posta elettronica, quando ciò appaia ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.