Allegato B) all'atto di nomina a Responsabile del trattamento dei dati (approvato con Decreto Commissariale n.17 8/2018)

REGIONE DEL VENETO
AZIENDA ZERO

Regolamento

per l'utilizzo delle risorse ICT

(Information and Communication Technology)

Indice

1 Introduzione

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone l'Azienda Zero e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità conseguenti alla violazione di specifiche disposizioni normative creando problemi alla sicurezza e alla immagine dell'azienda.

Posto che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, e che tutte le risorse ICT (Information and Communication Technology), fornite dall'Amministrazione agli Utenti, come definiti al paragrafo 1.1, devono essere utilizzate in modo appropriato, efficiente, rispettoso e per motivi lavorativi, Azienda Zero adotta il presente regolamento interno al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.

Considerato inoltre che Azienda Zero, nell'ottica di uno svolgimento più agevole della propria attività, mette a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti *(computer portatili, tablets, telefoni cellulari, smartphone, etc*.), sono state inserite nel regolamento alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di detta strumentazione.

1.1 Definizione delle risorse ICT

Le risorse ICT, messe a disposizione da Azienda Zero, oggetto di tutela da parte del presente documento, sono:

- il patrimonio informativo di cui al paragrafo 3, detenuto dall'Amministrazione, in formato elettronico;
- i servizi informatici erogati dall'Amministrazione;
- le postazioni di lavoro "fisse" (PC desktop e simili) e "mobili" (PC portatili e simili);
- i dispositivi cellulari (*smartphone*);
- i software di comunicazione (tipo "*messenger*" e simili);
- *i server*, le apparecchiature e tutto il materiale *hardware* in generale.

1.2 Finalità del presente documento

Il presente documento si prefigge di tutelare le risorse ICT dell'Amministrazione e di fornire indicazioni agli Utenti circa il corretto ed appropriato uso delle stesse.

L'Amministrazione, in particolare, intende perseguire i seguenti obiettivi:

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;
- garantire il rispetto della normativa in materia.

1.3 Contesto Normativo di riferimento

Questo documento fa riferimento al seguente quadro normativo:

- "*Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "**GDPR**");
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"(d'ora in poi "**Codice**");
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008).
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

1.4 Ambito di applicazione del presente documento

Il presente documento si applica ai soggetti di seguito indicati e, per brevità, definiti "Utenti":

a) Direttori e dipendenti, a qualsiasi titolo inseriti nell'organizzazione aziendale, senza distinzione di ruolo e/o livello;
b) consulenti e collaboratori dell'Azienda, a prescindere dal rapporto contrattuale intrattenuto con la stessa;
c) dipendenti e collaboratori di società che hanno un contratto in essere con l'Azienda e che utilizzano risorse ICT della stessa;
d) ospiti dell'Azienda, per l'eventuale uso delle risorse ICT della stessa;
e) Enti e Agenzie attestati alla rete Intranet, per quanto applicabile.

Le norme si rivolgono a differenti categorie di soggetti essendo destinate a disciplinare sia il comportamento di Utenti "meri utilizzatori" (fruitori di PC desktop, smartphone, PC

portatili, ecc.), sia il comportamento di Utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.).

Ciascun Utente, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, rivolgersi all'UOC Sistemi Informativi.

2 Regole per il corretto uso delle risorse ICT

2.1 Premessa

Le regole sono declinate su tre versanti: organizzativo, tecnologico-procedurale e comportamentale.

Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dell'Amministrazione.

In particolare:

- La confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- l'integrità è relativa alla completezza ed inalterabilità delle informazioni;
- la disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

2.2 Soluzioni organizzative

Ciascun Responsabile del trattamento dei dati personali designa un ***Referente Privacy*** all'interno della propria struttura e segnala il nominativo all'UOC Sistemi Informativi.

Il Referente esamina le questioni correlate all'applicazione della normativa sulla privacy e tiene i contatti con l'UOC Sistemi informativi.

2.2.1 Gestione degli incidenti e databreach

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato dall'Utente in modo tempestivo all' dell'UOC Sistemi Informativi , che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Nel caso l'incidente di una certa gravità riguardi il patrimonio Informativo e di conoscenza detenuto dall'Azienda oppure le applicazioni informatiche, l'Utente dovrà avvisare anche il Direttore dell'UOC di riferimento/appartenenza e il Direttore dell'UOC Sistemi informativi

Per gli incidenti che possono determinare una violazione dei **dati personali**, *cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati* (cd. "***databreach***")"l'art. 33 del GDPR prevede che in caso di violazione dei dati personali, "*il titolare del trattamento notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*.

Il successivo art. 34 disciplina il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare la violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo:

a) *il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
b) *il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;*
c) *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

Per ottemperare agli obblighi imposti dalla norma ogni Utente, avvisa senza indugio l'UOC Sistemi informativi, segnala anche al proprio Direttore le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali. Il Direttore/Responsabile dei dati avvisa l'UOC Sistemi informativi e, unitamente, procedono alle comunicazioni del l'avvenuto incidente di databreach e all'avvio dell'istruttoria per la comunicazione all'interessato.

2.2.2 Autenticazione Utenti

L'accesso a tutti i servizi deve avvenire previa procedura di autenticazione.

Gli Utenti devono essere identificati e ricevere dal gestore del servizio delle credenziali individuali (*nome utente* e *password*), che devono essere mantenute riservate e custodite con cura. Ogni *password* deve essere associata esclusivamente ad un unico soggetto identificato.

Le credenziali, laddove utilizzate, non possono essere assegnate ad altri Utenti, neppure in tempi diversi.

Le credenziali non utilizzate da almeno tre mesi sono disabilitate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Il gestore può, a fronte di particolari situazioni, sospendere o disabilitare le credenziali rilasciate (pensionamento, dimissioni ecc.)

Gli Utenti devono proteggere le credenziali memorizzate sugli *smartphone*, tablet e p.c. utilizzati per fruire dei servizi dell'Azienda (ad es. posta elettronica, intranet, ecc.) e, nel caso di furto o smarrimento siano essi personali o dell'Azienda, devono cambiare tempestivamente la "*password del dominio*" .

2.2.3 Autorizzazione e profilatura degli Utenti

Le credenziali di autenticazione per l'accesso ai sistemi e alle procedure aziendali vengono assegnate dal personale del l'UOC Sistemi informativi o da altro personale appositamente incaricato, previa formale richiesta del Responsabile dell'unità operativa nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Nel caso di collaboratori la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile della unità operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico. Lo stesso dicasi nel caso di revoca e/o trasferimento.

Gli Utenti, precedentemente autenticati, devono essere autorizzati dal gestore (responsabile) del servizio circa l'ambito di accesso/conoscenza del Patrimonio Informativo dell'Azienda e le operazioni che su di esso possono eseguire.

Sarà cura del Direttore della struttura in cui opera l'Utente chiedere al gestore (responsabile) del servizio di assegnare e/o modificare i diritti di accesso al servizio medesimo, in base alle mansioni assegnate e svolte dall'Utente.

2.2.4 Sicurezza dei server

I gestori di *server* devono configurare i *server* medesimi conformemente agli standard di sicurezza e/o *best practices* (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le "*pacth*", ecc.) emessi da Enti ed Organizzazioni internazionali (ad es. *International Standard Organization* - ISO, *National Institute of Standards and Technology* - NIST, *Sans Intitute*, ecc.)

Laddove le strutture si avvalgano di propri fornitori dovranno prevedere nei contratti di appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovranno prevedere clausole di "responsabilità esterna" e di "amministrazione dei sistemi", in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25.06.2009.

2.2.5 Sicurezza delle applicazioni

Le strutture che sviluppino applicazioni informatiche devono rispettare l'approccio della "*privacy by design*", incorporando sia i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni[1] che, per le applicazioni *webbased*, le *best practices* emesse dall'Organizzazione internazionale Open Web Application Security Project (OWASP);

Il GDPR, al 78° "considerando" iniziale stabilisce che: " *in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della* ***protezione dei dati fin dalla progettazione*** *e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici*."

Le strutture aziendali, qualora affidino ad un fornitore l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto il rispetto delle stesse prescrizioni di cui al precedente punto.

Sarebbe opportuno, inoltre, prestare analoga attenzione anche nel caso di applicazioni acquistate sul mercato (c.d. applicazioni <<COTS>> "*Commercial Off-the-Shelf component*").

2.2.6 Sicurezza della rete

l'UOC Sistemi Informativi configura la Rete Telematica dell'Azienda per contribuire alla protezione dei server, che dovranno essere collocati su sottoreti dedicate e con strumenti e livelli di protezione (ad es. *firewall, IPS, application firewall*, ecc.) adeguati in base al livello di classificazione assegnato ai dati ospitati nei server medesimi.

2.2.7 Gestione della disponibilità (salvataggio e ripristino dei dati)

Tutte le strutture aziendali che hanno presso le proprie sedi server gestiti in proprio devono prevedere un processo di "*backup"* e "*restore"* dei dati in modo da garantire la disponibilità dei dati, mitigando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella gestione dei dati.

---

[1] Ad es. gli applicativi, di *default*, non devono consentire la conoscibilità delle informazioni a chiunque, ma devono consentire agli Utenti ambiti di operatività non eccedenti rispetto al profilo di appartenenza.

2.2.8 Gestione dei *log file*

Tutte le strutture aziendali che hanno presso le proprie sedi server gestiti in proprio devono attivare un sistema di raccolta delle informazioni relative all'accesso ai dati, sistemi, reti ed applicazioni utilizzati dall'Amministrazione, in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema) come modificato con successivo Provvedimento Generale del 25.06.2009.

2.2.9 Gestione delle caselle di posta elettronica

Fatto salvo quanto previsto in seguito circa l'utilizzo del servizio di Posta Elettronica dell'Azienda, ad ogni Utente viene assegnato un determinato spazio per la memorizzazione sul server centrale di posta.

Esaurito il predetto spazio sul server, l'Utente potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione o lo "*scarico*" dei messaggi di posta.

Una copia di tutti i messaggi di posta elettronica "in arrivo" e in partenza, presenti sul server, è salvata con procedure di "*backup*" a cadenza giornaliera per un periodo di 21 giorni consecutivi.

Qualora l'Utente "*scarichi*" sulla propria postazione di lavoro ovvero cancelli i messaggi di posta ancora presenti sul server, tali messaggi non saranno oggetto di "*backup*".

2.2.10 Gestione delle richieste di accesso al contenuto di risorse ICT

L'Azienda in caso di Utenti deceduti, sospesi o cessati dal servizio, potrebbe avere la necessità di recuperare documenti importanti su risorse ICT, assegnate ai predetti Utenti, al fine di proseguire le attività in cui gli Utenti medesimi erano coinvolti.

In tali casi il Direttore della Direzione o dell'Area di afferenza dell'Utente assegnatario delle risorse ICT potrà chiedere al Direttore dell'UOC Sistemi Informativi di avere accesso alle suddette risorse ICT per estrarre dalle risorse medesime le informazioni indispensabili per proseguire l'attività lavorativa.

2.3 Soluzioni comportamentali

2.3.1 Uso delle risorse e fruizione del wifi

Tutti gli Utenti devono utilizzare le risorse ICT, fornite dall'Amministrazione, in maniera diligente, in modo appropriato, efficiente, rispettoso e per motivi lavorativi.

Gli Utenti devono utilizzare le risorse ICT solamente per fini professionali (in relazione alle mansioni assegnate) e per conto dell'Azienda, evitando l'uso per attività non pertinenti (ad esempio esecuzione di programmi di intrattenimento, giochi *on line*, etc.).

Al fine di scongiurare i rischi derivanti dall'effetto "*bridge*" (ponte) tra la rete Intranet aziendale ed altre reti, gli Utenti devono evitare di accedere dall'esterno della rete Intranet ai servizi di posta elettronica aziendali e/o al servizio web aziendale e contemporaneamente ad altri siti Internet potenzialmente pericolosi.

Particolare cautela deve essere posta, inoltre, nella utilizzo di reti wifi gratuite per accedere alla rete Intranet e ai servizi di posta elettronica aziendale dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite da malintenzionati/hacker.

Gli Utenti non devono eseguire copie (anche parziali) di software protetto da leggi sul diritto d'autore che sia installato sui dispositivi forniti in uso dall'Amministrazione.

Gli Utenti sono tenuti a:

- sottoporre a scansione antivirus preventiva gli eventuali supporti mobili utilizzati (pendrive USB, CDROM/DVD, hard disk esterni, ecc.) prima di utilizzare le risorse negli stessi contenuti;
- modificare periodicamente le password, con le modalità previste dalle procedure indicate al punto 5 dell'Allegato B al D.Lgs. 196/2003 e con cadenza almeno trimestrale;
- presidiare le risorse ICT al fine di evitare l'accesso a soggetti terzi non autorizzati;
- bloccare i dispositivi connessi alla rete nel caso in cui non si possano presidiare i dispositivi medesimi;
- non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione;
- procedere allo spegnimento delle postazione di lavoro "fisse", al termine dell'orario di lavoro, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento.

2.3.2 Utilizzo di dispositivi cellulari e computer portatili.

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di dispositivi cellulari e computer portatili, all'esterno dei locali dell'Azienda, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti.

Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "*infettati*" da virus o codice malevole.

Per altro un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Amministrazione, una volta che tali dispositivi siano collegati direttamente alla rete interna.

E' necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- fare periodicamente delle copie di *back-up* dei dati e verificarle regolarmente;
- attestarsi, con frequenza almeno settimanale, alla rete intranet dell'Azienda per scaricare gli aggiornamenti forniti dall'Amministrazione (*patch*, *hot fix* ed elenchi dei virus);
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate dall'Amministrazione;
- evitare di accedere e navigare in siti *web* "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il *bluetooth*, oltre il tempo strettamente necessario.

2.3.3 Modifiche delle risorse ICT

Per quanto riguarda le modifiche si devono distinguere:

a) modifiche *hardware* degli strumenti dell'Amministrazione: gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo od installando componenti

hardware (ad esempio masterizzatori CDROM/DVD, schede LAN, ecc.) senza autorizzazione dell'UOC Sistemi Informativi;

b) modifiche *software*: gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione della l'UOC Sistemi Informativi. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze negative sulla funzionalità dei dispositivi stessi. Gli Utenti, inoltre, non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) senza autorizzazione dell'UOC Sistemi Informativi.

2.3.4 Smarrimento e furto delle risorse ICT

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, gli Utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:

a) Autorità Giudiziaria (sporgendo denuncia);

b) *Call Center* dell'Assistenza informatica, per l'eventuale blocco dell'uso delle risorse ICT;

c) Direttore della propria Struttura di appartenenza;

d) Direttore dell'UOC Informatica, mediante comunicazione formale.

3 Gestione dei Dati

Il patrimonio informativo e di conoscenza detenuto dall'Amministrazione si suddivide in due macroaree:

- dati personali;

- dati (*riservati o non riservati*) diversi da quelli personali.

Le due fattispecie necessitano di trattamenti peculiari, fatte salve le più generali cautele e misure di sicurezza descritte a proposito dei dispositivi come più sopra indicato.

3.1 I Dati personali

In questo paragrafo si vuole porre l'attenzione sugli aspetti di sicurezza relativi al trattamento di dati personali.

Ai fini della corretta applicazione delle indicazioni che seguono, si ritiene utile riportare di seguito la classificazione dei dati personali fatta dal legislatore.

Ai sensi dell'Art. 4 del GDPR, è un "***dato personale***", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

a) I dati personali devono essere trattati e protetti secondo quanto previsto dal GDPR e dal Codice.

b) i dati personali, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita,

anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

c) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

d) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

e) Specifiche misure di sicurezza (c.d. "misure minime" di sicurezza) sono prescritte dagli artt. 33-36 e Allegato B del Codice e, ai fini di questo documento, sono destinate ad Utenti diversi (gestore del servizio/sistema, direttore/responsabile del trattamento, utente/incaricato del trattamento). Ad es. spettano al gestore del servizio gli obblighi in tema di autenticazione informatica; al Responsabile del trattamento la nomina degli Incaricati e l'aggiornamento periodico dell'ambito di trattamento consentito; agli Incaricati del trattamento attenersi alle istruzioni ricevute con la nomina e adottare le necessarie cautele per la segretezza della *password*.

f) All'atto della dismissione di supporti che contengano dati personali è necessario distruggere o rendere inutilizzabili (*cancellandone il contenuto*) i supporti medesimi, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*".

3.1.1 Dati particolari/sensibili e giudiziari/ relativi a condanne penali e reati.

Tutti gli Utenti devono porre particolare attenzione nei trattamenti dei dati personali particolari/sensibili e giudiziari/ relativi a condanne penali e reati (definiti all'art. 9 del GDPR ed all'art. 4 del Codice) in relazione alla confidenzialità dei dati.

Sono indicati alcuni comportamenti o regole minime da rispettare: *cifrare i dati memorizzati sui file/database o in fase di trasferimento; proteggere i canali di trasmissione; evitare l'invio con la posta elettronica di dati sensibili e giudiziari; recuperare tempestivamente i documenti stampati o ricevuti via fax che contengano dati sensibili o giudiziari per sottrarli alla vista di chi non è autorizzato; separare logicamente i dati "comuni" da quelli sensibili/giudiziari nei database, ecc*.

3.2 I dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali (definiti al precedente punto 3.1) sono classificati in base al livello di Confidenzialità (*Confidentiality*) come segue:

1. Dati riservati
2. Dati non riservati.

3.2.1 Dati riservati

Appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà individuale, il diritto d'autore e i segreti commerciali).

La gestione, trasmissione e condivisione dei dati riservati deve essere sottoposta a particolari cautele e misure, stabilite dal soggetto responsabile, al fine di preservare la confidenzialità dei dati medesimi.

L’eventuale manutenzione, effettuata da partner privati, sui sistemi ed apparati che ospitano dati riservati deve essere disciplinata, a livello contrattuale, prevedendo specifici obblighi di riservatezza a carico dei partner privati.

3.2.2 Dati non riservati

Appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni (ad es. gli “*Open Data*”, i dati oggetto di “accesso civico”, ecc.)

Per i dati non riservati, il responsabile stabilisce le forme e modalità attraverso cui rendere disponibili e/o liberamente accessibili i dati nel rispetto della normativa vgente

4 Modalità e doveri nell’utilizzo di posta elettronica, internet, computer portatili, tablets, telefoni cellulari, smartphone

4.1 Posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Gli Utenti assegnatari delle caselle di Posta Elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti, in un’ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello “spam” (*trasmissione su larga scala e in grandi volumi di e-mail non sollecitati*).

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo quanto di seguito indicato.

In caso di necessità e urgenza, è possibile possono utilizzare la Posta Elettronica per motivi non attinenti all’attività lavorativa e, comunque, non in modo ripetitivo. In tali limitati casi, le e-mail personali è opportuno che siano contrassegnate con la menzione “Privato” o “Riservato” all’inizio dell’oggetto.

Ove possibile, ai fini di una migliore differenziazione tra e-mail private o riservate ed email professionali, gli Utenti potranno chiedere ai mittenti che eventuali e sporadici messaggi privati o riservati siano inviati con la dicitura “Privato” o “Riservato” nell’oggetto. Fermi restando i limiti generali di accesso da parte del Datore di lavoro alla posta elettronica messa a disposizione del lavoratore, all’Amministrazione non è consentito prendere visione delle e-mail che recano la menzione “Privato” o “Riservato”. In caso di controllo su base individuale e nominativa, allorché non ci sia distinzione fra Posta Elettronica privata e professionale e la natura privata di un messaggio non sia riconoscibile, l’Amministrazione presuppone che si tratti di Posta Elettronica professionale..

E’ fatto divieto, in ogni caso, di trasmettere a chiunque a mezzo Posta Elettronica materiale pedofilo/pornografico, materiale fraudolento/illegale, gioco d’azzardo, materiale blasfemo o molesto/osceno. Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La conservazione on line è garantita per 24 mesi.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da

inviarsi mediante gli strumenti tradizionali devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di unità operativa, a seconda del loro contenuto e dei destinatari delle stesse. Sono state attivate caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea.

È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o Ftp non conosciuti).

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura / servizio. In tal caso, la funzionalità deve essere attivata dall'utente.

Sarà comunque consentito al superiore gerarchico dell'utente accedere alla casella di posta elettronica dell'utente in caso di mancata attivazione della funzionalità di cui al punto sopra e in caso di assenza non programmata, qualora vi siano ragioni di servizio per l'accesso, tramite il personale dell'UOC Sistemi Informativi o altro personale esterno a ciò incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento.

Non è autorizzato l'utilizzo per fini istituzionali di indirizzi e-mail personali privati al di fuori del dominio aziendale.

4.2 Navigazione in internet

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa, salvo le indicazioni presenti nel successivo capitolo decimo.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda adotta uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list". L'azienda si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa e compatibili con le finalità non istituzionali di cui al successivo capitolo decimo.

Gli eventuali controlli, compiuti dal personale incaricato dell'UOC Sistemi Informativi, ai sensi del precedente punto 4.1, potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

L'utilizzo e la consultazione di social network sono permessi esclusivamente per finalità istituzionali e previa autorizzazione del Dirigente responsabile della unità operativa.

In caso di necessità e urgenza gli Utenti possono navigare in Internet per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.

E' consentita, previa autorizzazione del Dirigente responsabile della struttura, la consultazione occasionale di siti internet per finalità non istituzionali e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano

compatibili con le misure di sicurezza implementate a protezione del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi di servizio che il dipendente ha nei confronti dell'Ente.

L'utente utilizzatore del personal computer verifica periodicamente lo stato di aggiornamento dell'antivirus aziendale installato. A fronte di eventuali anomalie contatta l'UOC Sistemi Informativi

4.3 Utilizzo di telefoni, scanner e fotocopiatrici

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.

Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per I 'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l' addebito delle chiamate personali.

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa autorizzazione da parte del Responsabile dell'unità operativa.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.

È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.

Solo in caso di necessità e urgenza, gli Utenti possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.

Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Responsabile della unità operativa a cui detti strumenti sono stati assegnati.

4.4 Utilizzo di smartphone, tablet e relative applicazioni mobili (APP)

Premesso che i terminali di nuova generazione applicati alla telefonia mobile (smartphone e tablet) e le relative applicazioni mobili software (note comunemente con l'abbreviazione "App"), sono in fase di evoluzione costante e consentono, con crescente facilità, di utilizzare, registrare e trasmettere dati sensibili tramite diverse tecnologie di rete, comunicando e diffondendo in rete dati e immagini in tempo reale, si fa presente che si tratta di apparecchiature che, per le loro potenzialità, possono essere utilizzate violando, anche involontariamente, i diritti delle persone interessate alla comunicazione, come pure di terzi inconsapevoli.

Premesso ciò si definiscono per i casi seguenti le regole:

CASO 1 - Smartphone/Tablet aziendale in cui è richiesta l'installazione di una applicazione aziendale che gestisce dati sensibili: in questo caso l'autorizzazione per l'installazione è permessa solo se i dispositivi Smartphone/Tablet sono supportati da un apposito sistema di sicurezza aziendale

CASO 2 - Smartphone/Tablet aziendale in cui è richiesta l'installazione di una applicazione mobile App (aziendale) che gestisce dati sensibili: è autorizzata in questo caso l'installazione di App (aziendali) che gestiscono dati sensibili esclusivamente se tali App sono certificate come Dispositivi Medici secondo le norme e le direttive in vigore sui DM. Inoltre l'autorizzazione di installazione è permessa solo se i dispositivi Smartphone/Tablet sono supportati da un apposito sistema di sicurezza aziendale

CASO 3 - Smartphone/Tablet personali in cui è richiesta l'installazione o di una applicazione aziendale o di una applicazione mobile App che gestiscono dati sensibili: in questo caso non sono ammesse installazioni di applicazioni e/o App aziendali di nessun tipo.

5 Protezione antivirus

Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software di tipo malware

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l' accaduto all'UOC Sistemi Informativi.

Ogni dispositivo di supporto di memorizzazione elettronico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale dell'UOC Informatica.

L'utente utilizzatore del personal computer verifica periodicamente lo stato di aggiornamento dell'antivirus aziendale installato. A fronte di eventuali anomalie contatta il Servizio dell'UOC Informatica

6 Controlli

L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 (così detto *"Decreto sulle semplificazioni"* attuativo della Legge delega 10.12.2014 n. 183, anche nota come *"legge di riforma del diritto del lavoro"* o *"Jobs Act"*) ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato *"Impianti audiovisivi e altri strumenti di controllo".*

Il testo del nuovo articolo 4 della Legge 300/1970, nel confermare, al primo comma, la disciplina applicabile agli strumenti di controllo a distanza dell'attività dei lavoratori necessari per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (come le telecamere o i rilevatori di posizione Gps), che rimangono sottoposti alla stessa disciplina di divieti e di controlli di prima, ha introdotto, al comma due, una disciplina diversa per quanto concerne i dispositivi utilizzati dal lavoratore per rendere la prestazione lavorativa (computer, tablet, telefoni, smartphone) stabilendo espressamente che *"La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli*

accessi e delle presenze. Le informazioni raccolte a sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.lgs. 30 giugno 2003 n. 196

Alla luce delle disposizioni dettate dal succitato D.lgs. 151/2015, l'Azienda può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno effettuarsi i controlli.

Si dà atto che l'informativa ai lavoratori, di cui al precedente capoverso, viene garantita dall'Azienda mediante la diffusione del presente Regolamento, approvato con delibera del Direttore Generale/Commissario, e che le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro nel rispetto di quanto previsto dal "Codice della privacy" (D.lgs. 196/2003)

In ottemperanza a quanto stabilito dall'art. 4 del d.lgs. 300/1970, non vengono nel modo più assoluto utilizzate apparecchiature/strumentazioni hardware e software al fine di consentire controlli a distanza, prolungati, costanti o indiscriminati dei lavoratori. È quindi nel pieno rispetto dei principi di pertinenza e di non eccedenza ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, che l'Azienda si riserva di effettuare controlli sull'uso degli strumenti ICT. Detti controlli sono svolti esclusivamente dalla Struttura competente per la gestione dei sistemi informativi. I controlli effettuati di routine sono indiretti e di tipo aggregato. In particolare detti controlli sono finalizzati a verificare la funzionalità e la sicurezza dei sistemi. Controlli indiretti di tipo aggregato, ma più specifici, vengono altresì attivati in caso di rilevamento di anomalie nell'utilizzo delle apparecchiature ICT. Qualora la anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo si procederà con l'effettuazione di controlli più puntuali e su base individuale secondo le modalità indicate al successivo punto 7.

7 Graduazione dei controlli

Premesso che *"il dipendente deve utilizzare il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione"* (art. 11, Codice di comportamento dei dipendenti pubblici), come stabilito dal Garante della privacy nelle già citate "Linee guida per posta elettronica e internet" del 01.03.2007, all'articolo 6.1. rubricato "Graduazione", nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

Come stabilito altresì' dalla già citata Direttiva n. 2/2009 ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", l'eventuale controllo è lecito solo se sono rispettati i principi di proporzionalità, pertinenza e non eccedenza nelle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono essere proporzionate allo scopo perseguito ed è, in ogni caso, esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati.

Per quanto possibile deve essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

8 Utilizzo di social networks

Al fine di assicurare il rispetto del segreto d'ufficio, del segreto professionale e della riservatezza dei dati conosciuti in ambito aziendale, è vietato l'uso, anche privato, dei social networks per lo scambio di informazioni e dati inerenti l'attività istituzionale.

9 Conservazione

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari; all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate e dev'essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

10 Violazioni

L'eventuale violazione delle norme e/o delle buone regole di comportamento può comportare l'applicazione in capo ai contravventori di sanzioni di tipo civile, penale e/o disciplinare.

11 Entrata in vigore e pubblicità

Le regole contenute nel presente atto entrano in vigore dalla data di adozione del provvedimento di approvazione.

Del presente atto sarà fornita massima pubblicità e diffusione mediante la sua pubblicazione nel sito internet aziendale, nell'l'*intranet* aziendale e nell'A*ngolo del dipendente*

12 Disposizioni finali

Per quanto non espressamente richiamato nel presente atto, si rinvia alle disposizioni civili e penali vigenti in materia.