SOMMARIO

STATO	DATA	FIRMA
Verificato	01.03.2021	Dott.ssa L. Bortoluzzi
Approvato	01.03.2021	Dott.ssa C. Gibertoni
Approvato	01.03.2021	Ing. L. Capitani
Data di applicazione: 08.03.2021		

1.0 Oggetto e Scopo

La presente Istruzione Operativa ha lo scopo di disciplinare l'utilizzo della posta elettronica e di Internet, al fine di assicurare la funzionalità e il corretto impiego delle risorse stesse tenendo conto della disciplina in materia di diritti e libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali (art. 1, comma 2, Regolamento UE 2016/679), nonché della disciplina in tema di diritti e relazioni sindacali.

La previsione di regole di utilizzo delle risorse informatiche chiare e puntuali ha inoltre lo scopo di tutelare il lavoratore, consentendo al medesimo di organizzare la propria attività e gli strumenti del proprio lavoro secondo criteri idonei a garantire la sicurezza e la funzionalità degli strumenti stessi.

I rischi connessi alla crescente diffusione delle nuove tecnologie e l'impiego sempre più frequente di queste ultime all'interno della realtà aziendale, impongono di informare e istruire adeguatamente gli utenti circa l'utilizzo dei strumenti informatici aziendali, al fine di scongiurare il più possibile rischi di natura patrimoniale ed eventuali responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli autorizzati con i documenti Istruzione Operativa Aziendale in materia di protezione dei dati personali (IOA29), per brevità Codice Privacy e Regolamento Aziendale per l'utilizzo delle risorse informatiche, con particolare riferimento alla sicurezza e riservatezza (IOA44).

Il presente documento ha la finalità di stabilire le norme per l'accesso e l'utilizzo dei seguenti servizi:

1. Posta elettronica
2. Rete Internet

di seguito indicati nel loro complesso come "strumenti informatici aziendali".

L'utilizzo degli strumenti informatici aziendali deve ispirarsi al principio della diligenza e correttezza normalmente adottate nell'ambito dei rapporti di lavoro. L'Azienda deve garantire altresì la riservatezza dei dati trattati con strumenti informatici, evitando accessi impropri, garantendo la tracciabilità degli accessi ed evitare che la trasmissione del dato possa renderlo visibile a terze parti non autorizzate.

2.0 Campo di applicazione

Il presente documento si applica a tutti i dipendenti dell'Azienda e loro equiparati, ivi comprese le figure, pur non dipendenti, comunque autorizzate al trattamento dei dati (ad es. collaboratori esterni, fornitori, ecc.) alle quali, al momento dell'incarico, deve essere fornito il presente Documento, anche attraverso il link della pagina del sito internet aziendale nel quale è stato pubblicato.

3.0 Responsabilità

Gruppo di redazione: il documento è stato redatto dal gruppo di lavoro interaziendale costituito dagli Uffici Information and Communication Technology (ICT) e dagli Uffici Privacy, coordinati dal DPO che ne ha validato i contenuti. Il Servizio Information and Communication Technology (ICT) è responsabile del riesame e aggiornamento del documento.

4.0 DOCUMENTI DI RIFERIMENTO

Documento (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 (Documento generale sulla protezione dei dati), di seguito denominato "GDPR";
Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Documento (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", di seguito "Codice";
Legge 20 maggio 1970, n. 300 e successive modifiche ed integrazioni "Statuto dei lavoratori", di seguito denominato "Statuto";
Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche ed integrazioni "Codice dell'amministrazione digitale", di seguito CAD;
Provvedimento generale del Garante per la protezione dei dati personali del 1° marzo 2007 Delibera n. 13 "Lavoro: le linee guida del Garante per posta elettronica e internet", di seguito denominato "Linee Guida";
Direttiva 26 maggio 2009, n. 2 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri, di seguito denominata "Direttiva";
Decreto del Presidente della repubblica 11 febbraio 2005 n. 68 - AGID - "Documento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3";
Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013, "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d), numeri 1) e 2) del decreto-legge 13 maggio 2011, n.70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, recante «Semestre europeo - prime disposizioni urgenti per l'economia». (13A08392)".

PA05 "Procedura aziendale di controllo dei documenti del sistema qualità"

IOA29 "Documento aziendale attuativo delle disposizioni in materia di trattamento di dati personali"

IOA44 "Documento aziendale per l'utilizzo delle risorse informatiche, con particolare riferimento alla sicurezza e riservatezza" e relativi allegati

5.0 DEFINIZIONI

Ai fini di una corretta comprensione delle disposizioni del Documento, si ritiene opportuno elencare le seguenti definizioni:

- **trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **dato personale**: qualsiasi informazione riguardante una persona fisica, identificata o identificabile; 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;
- **dati particolari**: sono quei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale, o all'orientamento sessuale della persona;
- **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica il servizio o altro organismo che singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento dei dati personali;
- **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **autorizzato al trattamento**: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento;
- **interessato**: la persona fisica cui si riferiscono i dati personali;
- **credenziali di autenticazione**: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- **parola chiave (password)**: 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;
- **posta elettronica certificata (PEC)**: ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;
- **file log**: file generato automaticamente da un sistema software, che registra alcune operazioni che avvengono in fase di avvio o di esecuzione;
- **posta elettronica semplice (e-mail):** insieme delle procedure che permettono lo scambio di messaggi (prodotti con strumenti informatici) tra utenti che appartengono a una stessa rete di PC o a reti distinte, variamente collegate tra loro;

- **referente privacy (ex Responsabile interno del trattamento):** soggetto interno a cui sono affidati dal titolare del trattamento compiti, funzioni e responsabilità nell'applicazione della normativa privacy in considerazione della natura gestionale e della complessità delle strutture organizzative dirette;
- **utente:** deve intendersi ogni dipendente, collaboratore e ogni soggetto autorizzato comunque operante presso l'Azienda, il quale, in qualità di autorizzato al trattamento dei dati personali, deve attenersi alle istruzioni impartite dal Titolare e/o Responsabile del trattamento, nonché alle istruzioni di seguito specificate.

6.0 CONTENUTO

6.1 Autorizzazione al trattamento dei dati personali

Gli strumenti informatici sono strumenti di lavoro forniti dall'Azienda, la quale fissa le modalità di utilizzo che gli utenti sono tenuti ad osservare scrupolosamente.

Gli utenti sono autorizzati, ai sensi del GDPR, al trattamento dei dati ai quali hanno accesso o che sono trattati mediante gli strumenti informatici aziendali secondo le disposizioni di cui al documento Istruzione Operativa Aziendale in materia di protezione dei dati personali (IOA29).

Gli utenti, in ogni caso, possono trattare i dati limitatamente alle operazioni indispensabili per le finalità per i quali sono stati raccolti e nei limiti delle funzioni loro attribuite, e comunque nel rispetto dei principi di cui all'art. 5 del GDPR (vedere anche Informativa sul trattamento dei dati personali agli utenti che utilizzando gli strumenti informatici aziendali T01/IOA99).

6.1.1 Finalità e limitazioni d'uso

L'accesso agli strumenti informatici aziendali è da intendersi quale "strumento di lavoro" e può pertanto essere effettuato nei limiti di quanto necessario per lo svolgimento della propria attività e delle proprie mansioni.

È pertanto vietato l'uso di tali strumenti per l'utilizzo di procedure aziendali con modalità e finalità non attinenti ai propri doveri d'ufficio e in generale per finalità incompatibili con i fini istituzionali dell'Azienda.

6.2 Assegnazione e gestione delle credenziali di autenticazione

L'accesso e l'utilizzo degli strumenti informatici aziendali sono subordinati al possesso da parte degli utenti di credenziali di autenticazione che vengono assegnate – secondo quanto specificato nei documenti Allegato 1/IOA44 "Regole e comportamenti per il corretto rilascio/rinnovo delle credenziali aziendali" e T02/IOA44 "Modalità di rilascio/scadenza/rinnovo delle credenziali aziendali ai soggetti delle categorie 1, 2, 3" – nel momento in cui lo stesso acquisisce il titolo che gli consente di accedere agli strumenti informatici aziendali (ad es. stipula di contratto, sottoscrizione di convenzione, ecc.).

Le proprie credenziali di autenticazione, che consistono in un codice per l'identificazione dell'utente (*user id*) associato ad una parola chiave segreta (*password*), rimangono in possesso ed uso esclusivo dell'utente.

La *user id* identificativa dell'utente è composta di norma dal nome e dal cognome dell'utilizzatore intervallati da un "." (ad esempio: mario.rossi).

Per l'accesso alle procedure sanitarie vengono assegnate anche credenziali con *user id* identificativa formata da lettere e numeri (ad esempio: SP12345), generalmente chiamate "credenziali SSO".

La *password* (impostata di default provvisoriamente e da cambiare obbligatoriamente al primo accesso) deve essere composta da almeno 10 caratteri che devono contenere, per ragioni di sicurezza, lettere maiuscole, lettere minuscole, caratteri speciali e/o numeri.

Nel caso in cui l'utente perda la qualità che gli consentiva di accedere agli strumenti informatici aziendali (ad es. cessazione rapporto contrattuale con fornitore, licenziamento del dipendente, ecc.) la credenziale di accesso viene disabilitata e non potrà essere riassegnata ad altro utente. Non sono previsti codici di accesso impersonali, salvo casi in cui sia prevista una successiva procedura di identificazione personale per l'accesso alle procedure e/o ai dati veri e propri, e salvo utilizzi per esigenze di natura tecnica e sistemistica.

Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia *user id* e *password* sarà attribuita in termini di responsabilità all'utente titolare del codice *user id*, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. L'utente non deve lasciare incustodita o facilmente accessibile la postazione di lavoro una volta collegata al sistema, e deve disattivare la connessione qualora si debba allontanare.

Le credenziali di autenticazione, in qualunque forma assegnate, dovranno essere custodite dall'utente con la massima diligenza e riservatezza e non dovranno essere divulgate né cedute, neppure temporaneamente, a terzi. Al fine di evitarne usi illeciti, le credenziali non devono essere memorizzate all'interno degli applicativi.

Nel caso in cui l'utente perda la qualità che gli consentiva di accedere agli strumenti informatici aziendali (ad es. alla scadenza del contratto di lavoro o di collaborazione o di fornitura con l'Azienda), le credenziali di autenticazione devono essere disattivate automaticamente alla scadenza del contratto dal Servizio ICT con effetto immediato.

L'Azienda si riserva, a seguito di evoluzione delle tecnologie, di introdurre, anche solo in particolari contesti, sistemi di autenticazione "forte", nel rispetto delle normative vigenti.

6.2.1 Password

La *password* non deve essere banale e contenere riferimenti agevolmente riconducibili all'utente. È necessario procedere alla modifica della *password* a cura dell'utente al primo utilizzo e, successivamente ogni 3 mesi. La stessa *password* non può essere riutilizzata nell'arco dei 18 mesi (corrispondenti a 6 cambi password successivi).

Alla scadenza dei 3 mesi, nel caso in cui l'utente non abbia provveduto a modificare la propria *password*, la sua abilitazione verrà sospesa. L'utente avrà 2 mesi ulteriori per riattivare il proprio profilo, semplicemente cambiando la *password* con le modalità opportune e in modo autonomo. Alla scadenza dei 2 mesi ulteriori lo *user id* verrà disattivato.

La *password* deve essere mantenuta segreta e deve essere obbligatoriamente modificata dall'utente nel caso in cui egli abbia fondati sospetti che la segretezza della password sia venuta meno.

L'utente si impegna a comunicare immediatamente al Servizio ICT (assistenza.password@aosp.bo.it o interno 051 2143917) l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della *password*, al fine di valutare le azioni da intraprendere.

6.3 Disciplina e qualificazione della casella di posta elettronica semplice

La casella di posta elettronica semplice assegnata all'utente è espressione dell'organizzazione datoriale e costituisce uno strumento di lavoro teso a favorire sia una forma di comunicazione agile, di carattere informale ed operativo, sia la comunicazione ufficiale di documenti per via telematica in sostituzione quanto più possibile della comunicazione formale cartacea.

A richiesta del Referente Privacy della struttura, possono essere assegnate due tipologie di account di posta elettronica:

a) account di servizio, il cui nome richiama il servizio in cui lavora l'utente;
b) account legati al nominativo dell'utente richiedente.

A tutti i dipendenti l'Azienda, al momento dell'assunzione o dell'instaurazione del rapporto di lavoro, fornisce l'account di cui alla predetta lett. b). Tutti i possessori di una casella di posta elettronica nominativa sono tenuti a consultare quotidianamente la propria corrispondenza e sono responsabili del corretto utilizzo della stessa. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Con i messaggi di posta elettronica si possono inviare file allegati di dimensione massima di circa 37 MB.

Ogni account nominativo di posta ha a disposizione uno spazio dedicato di 10 GB. Il raggiungimento di tale limite implica l'impossibilità di utilizzare, in tutto o in parte, il servizio. Il raggiungimento del 90% dell'occupazione dello spazio disponibile viene segnalato all'utente mediante un messaggio di posta elettronica. Gli utenti possono

richiedere al Servizio ICT (assistenza.mail@aosp.bo.it) l'estensione dello spazio dedicato. Il Servizio ICT, previa istruttoria sulla ragione addotta dal richiedente, valuta se procedere e, in caso affermativo, provvede all'assegnazione di una diversa dimensione dello spazio dedicato alla posta.

L'account di servizio deve comunque essere associato ad almeno un altro account nominativo di utente e non può essere utilizzato per l'invio di messaggi, ma solo in ricezione. Sarà compito del Servizio ICT fare in modo che i messaggi inviati a detto indirizzo siano smistati a tutti gli appartenenti al gruppo a cui è associato l'account di equipe.

Gli utenti sono tenuti ad utilizzare, per le comunicazioni aziendali, esclusivamente l'indirizzo di posta elettronica aziendale. Pertanto, in linea con le raccomandazioni contenute nelle Linee Guida del Garante per la protezione dei dati personali, non può crearsi un'aspettativa di confidenzialità del contenuto, in capo all'utente o ai terzi, rispetto a tale forma di comunicazione, che potrà essere inoltrata e/o utilizzata per motivi attinenti all'attività lavorativa.

Al fine di rendere edotti i destinatari della natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi. A tal fine, nei messaggi di posta elettronica inviati il sistema inserirà il testo ivi riportato:

Avvertenze ai sensi del Documento Generale UE 679/2016

Il presente messaggio non ha natura di comunicazione personale da parte del mittente.

Le informazioni contenute in questo messaggio e nei suoi eventuali allegati sono riservate e per uso esclusivo del destinatario. Il ricevente se diverso dal destinatario, è avvertito che qualunque utilizzazione, divulgazione o copia di questa comunicazione comporta violazione delle disposizioni in materia di protezione dei dati personali ed è pertanto rigorosamente vietata e come tale verrà perseguita anche penalmente. Se non siete i destinatari del messaggio o lo avete ricevuto per errore, Vi preghiamo di darcene comunicazione e di rimuovere il messaggio stesso e gli allegati dal Vostro sistema.

Grazie per la collaborazione

È vietato l'utilizzo dell'account di posta elettronica aziendale per comunicazioni estranee all'attività lavorativa.

È consentito un moderato e circoscritto utilizzo di provider esterni di posta elettronica per comunicazioni personali, esclusivamente in modalità web, con l'avvertenza che l'Azienda non può fornire supporto in caso di impossibilità di raggiungere i siti web di

tali provider a causa delle particolari configurazioni della rete finalizzate a massimizzare la sicurezza.

6.3.1 Gestione della casella di posta elettronica in caso di assenza

In caso di eventuali **assenze programmate** dall'utente (ad es. ferie, attività di lavoro fuori sede, comando, ecc.), al fine di garantire la funzionalità del servizio di posta elettronica aziendale, si raccomanda all'utente di attivare l'opzione di invio automatico di un messaggio di risposta contenente l'indicazione di un altro indirizzo di posta elettronica aziendale cui fare riferimento o al quale il messaggio sarà automaticamente inoltrato, indicando eventualmente altre utili modalità di contatto della struttura. Nel caso in cui l'utente intenda avvalersi di questa funzionalità può, laddove non riesca a provvedere autonomamente, chiedere supporto al Servizio ICT (assistenza.mail@aosp.bo.it). Qualora l'utente sia assente per comando, l'account viene mantenuto ma viene temporaneamente sospeso l'accesso/utilizzo della mail aziendale.

In caso di eventuali **assenze non programmate** (ad es. per malattia), qualora l'utente si trovi nell'impossibilità di attivare la funzionalità di risposta automatica, il Servizio ICT (assistenza.mail@aosp.bo.it) potrà, su richiesta del Referente Privacy, disporre direttamente l'attivazione di analoghi accorgimenti laddove ciò si rendesse necessario al fine di garantire la continuità dell'attività aziendale. In tal caso all'utente verrà data pronta comunicazione circa l'attività svolta in sua assenza, al primo momento utile e al più tardi al suo rientro.

Qualora risulti indispensabile e/o indifferibile accedere alla casella e-mail in dotazione all'utente, per cause di forza maggiore derivanti da esigenze improrogabili legate alla continuità dell'attività lavorativa, ad esigenze di sicurezza ed operatività dello stesso sistema informatico, l'Azienda può accedere alla casella di posta elettronica aziendale assegnata all'utente per il tramite di un collega indicato dall'utente stesso, anche telefonicamente, ed estrarre copia dei messaggi attinenti l'attività lavorativa. In tutti i casi in cui si rendesse necessario accedere alla casella di posta elettronica aziendale per le predette attività, le contingenze non consentissero all'Azienda di raggiungere tempestivamente l'utente per l'indicazione di un collega che vi proceda, l'accesso sarà consentito al Referente Privacy di afferenza affinché lo stesso possa procedere, congiuntamente al supporto tecnico del Servizio ICT all'uopo incaricato, alla verifica del contenuto dei messaggi di posta elettronica inviati e ricevuti per mezzo dell'account di posta elettronica. Effettuata la verifica il Referente Privacy provvederà ad inoltrare i messaggi di posta e relativi allegati, rilevanti ai fini della contingenza e della continuità dell'attività svolta dall'utente. Le predette attività verranno documentate attraverso la redazione di un sintetico verbale che attesti le operazioni svolte, e all'utente verrà data pronta comunicazione circa l'attività svolta in sua assenza, al primo momento utile e al più tardi al suo rientro.

6.3.2 Accesso alla configurazione della casella di posta elettronica per ragioni di sicurezza o manutenzione

Quando motivi di sicurezza o di manutenzione lo richiedono, l'amministratore di sistema specificamente autorizzato per iscritto, anche con delega generale, previo avviso agli utenti interessati e anche in assenza di questi, può accedere alla configurazione delle caselle di posta elettronica per le sole finalità di sicurezza e manutenzione, per esclusive finalità tecniche. L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere risolto. In quest'ultimo caso, l'avviso all'utente deve essere rinnovato prima dell'accesso ai messaggi contenuti nella casella, fermo restando che l'accesso dell'amministratore di sistema può avvenire esclusivamente per motivi di sicurezza o manutenzione come sopra precisato.

L'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta, nel caso eccezionale di cui al periodo che precede), deve essere in ogni caso comunicata all'utente senza ingiustificato ritardo al termine dell'intervento.

Il servizio ICT dovrà annotare, anche in modalità telematica, gli interventi svolti, specificando i motivi, la data e l'orario dell'intervento, dando atto degli avvisi intervenuti nei confronti degli utenti.

6.3.3 Trasmissione informatica di dati relativi alla salute

La trasmissione dei dati personali è a tutti gli effetti un tipo di "trattamento", pertanto è soggetta ai vincoli di riservatezza e tracciabilità.

La posta elettronica semplice (e-mail) non è uno strumento sicuro per la trasmissione dei dati relativi alla salute e in generale ai c.d. dati particolari. La trasmissione avviene infatti "in chiaro", senza garanzia di confidenzialità dei contenuti e potenzialmente intercettabile sia nelle comunicazioni verso destinatari interni all'Azienda che esterni. Non ha pertanto le garanzie di sicurezza tali da renderla formalmente adeguata per la trasmissione di tali dati (anche perché accessibile dall'esterno della struttura tramite qualsiasi PC, tablet o smartphone collegati a Internet).

Quando non sia possibile ovviare in altro modo e si necessiti di una comunicazione di dati particolari, è fatto obbligo l'utilizzo di particolari accorgimenti di protezione dei contenuti e degli allegati (cifratura), o di servirsi di uno strumento alternativo di trasmissione alla posta elettronica. A tale proposito, si ricorda che la posta elettronica certificata, in modo predefinito e sicuro, trasmette i contenuti del messaggio inviato in forma crittografata e assolve già a questa prescrizione.

È opportuno ricordare che tali vincoli sussistono solo nel caso in cui la trasmissione sia relativa a dati personali. Questo implica che è consentita qualsiasi trasmissione per e-

mail aziendale che riporti riferimenti non espliciti a persone fisiche (ad es. link a documenti su applicativi aziendali, iniziali cognome e nome, n. pratica, ecc.).

In relazione alle modalità di consegna ai cittadini dei referti e in generale della documentazione sanitaria da parte delle Aziende, si rinvia alle disposizioni di cui al DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 8 agosto 2013, alle Linee Guida in tema di referti on-line del Garante per la protezione dei dati personali 25 giugno 2009 e alla disciplina nazionale e regionale in tema di Fascicolo Sanitario Elettronico (FSE).

In merito agli accorgimenti tecnici per la trasmissione sicura di dati particolari, ulteriori indicazioni operative sono fornite nella Istruzione Operativa Aziendale in materia di protezione dei dati personali (IOA29), paragrafo "Modalità di utilizzo del FAX/E-MAIL/FOTOCOPIATRICE/STAMPANTE".

Per la trasmissione di dati genetici si rimanda alla normativa specifica e si raccomanda il confronto con l'Ufficio Privacy e, per gli aspetti di natura tecnica, con il Servizio ICT.

6.3.4 Comunicazioni di massa

È fatto obbligo agli utenti segnalare al Servizio ICT l'eventuale ricevimento di messaggi, sia da utenti interni che esterni, appartenenti ad una delle seguenti categorie:

- "mail spamming" e "catene di S. Antonio";
- aventi contenuto diffamatorio per l'Azienda o i suoi dipendenti;
- aventi contenuto moralmente deplorevole, scandaloso, propagandistico per correnti politiche o fazioni religiose;
- aventi contenuto non attinente l'attività lavorativa ed il cui ricevimento sia "non gradito" all'utente;
- aventi il fine di "intasare" le caselle di posta elettronica.

La segnalazione, in caso di dubbi, va indirizzata esclusivamente via e-mail all'indirizzo assistenza.mail@aosp.bo.it, inoltrando l'e-mail sospetta.

Gli utenti interni che attuano uno dei comportamenti vietati verranno segnalati al Responsabile di afferenza per le eventuali sanzioni disciplinari.

Per quanto riguarda comunicazioni da inviare in maniera massiva a tutte le caselle di posta aziendali, in genere per comunicazioni che rivestono particolare importanza per un congruo numero di utenti, l'autorizzazione deve essere ottenuta dall'UO Comunicazione ed Ufficio Stampa (tutti@aosp.bo.it) che valuterà e approverà il testo proposto per l'invio.

6.3.5 Tempo di conservazione dell'account e del contenuto delle mail dopo la cessazione del rapporto di lavoro

Come già specificato all'Art. 4, in caso di cessazione del rapporto di lavoro o, in generale della perdita del titolo di accesso agli strumenti informatici l'account viene disattivato immediatamente.

Su richiesta dell'utente validata dal Referente Privacy, è consentito il mantenimento dell'account aziendale in modalità di sola ricezione – per un periodo massimo di 1 mese – con attivazione, a cura del Servizio ICT, di un messaggio di risposta automatica contenente l'indirizzo mail a cui scrivere per comunicazioni riferite al singolo utente, nonché l'account di servizio (se esistente) o altro account personale, relativamente alle comunicazioni di lavoro.

In tutti i casi in cui l'account venga disattivato, la casella e il relativo contenuto, costituendo patrimonio aziendale, rimarranno nella piena disponibilità della stessa per un periodo di 6 mesi dalla risoluzione del rapporto lavorativo trascorso il quale i messaggi verranno cancellati.

6.4 Casella di posta elettronica certificata (PEC)

La casella PEC può essere integrata nell'applicativo di gestione documentale assegnata per l'utilizzo nel sistema di protocollo aziendale (BABEL) o utilizzata per la corrispondenza che richieda particolari garanzie in merito all'invio e alla consegna della corrispondenza (CAD art. 48).

La PEC viene attribuita esclusivamente alla struttura di afferenza. Non vengono, pertanto, assegnate caselle PEC nominative ai professionisti.

Nel caso in cui una sola persona sia abilitata all'accesso alla casella di struttura si parla di casella monoutenza. Se la casella di struttura è multiutenza più persone possono essere abilitate all'accesso mediante credenziali personali.

La richiesta di attivazione della casella PEC va presentata al Servizio ICT mediante modulo R01/IOA99 "Richiesta creazione casella PEC aziendale".

6.5 Navigazione in Internet

La rete aziendale consente l'accesso alla rete Internet dalla maggior parte delle postazioni di lavoro interne all'Azienda (potrebbero essere escluse postazioni che, per particolari requisiti di sicurezza e criticità, sono mantenute isolate). È vietato l'utilizzo di accessi internet mediante Internet Provider diversi da quello scelto ufficialmente dall'Azienda e la connessione di stazioni di lavoro aziendali alle reti di detti Provider, anche con abbonamenti privati.

L'accesso alla rete Internet è consentito nell'ambito dello svolgimento delle proprie attività professionali. Non è consentito l'uso a scopo personale.

L'utente non potrà quindi utilizzare Internet, a titolo meramente esemplificativo e non esaustivo, per:

a) il download di programmi ancorché gratuiti, nonché l'utilizzo di documenti a carattere personale;
b) transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati;
c) ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
d) partecipazione a Forum non professionali, l'utilizzo di chat line e social network, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati dal Referente;
e) l'utilizzo di applicativi per l'ascolto della musica e/o la visione di video su siti se non espressamente autorizzati dal Referente in quanto necessario per lo svolgimento delle proprie mansioni.

A tale fine l'Azienda limita l'accesso alle risorse Internet sulla base di specifici sistemi di blocco automatico che prevengono l'accesso a determinati siti inseriti in una black list e come tali preventivamente classificati come non accessibili dall'utente. I suddetti filtri sono applicati verso alcuni siti web (ad es. sono esclusi siti classificati come pornografici, gioco online, trading online, ecc.) e sulla fruizione di specifici servizi (ad es. sono esclusi servizi di accesso ai social, download di software o di file musicali streaming audio e video). Qualora alcuni siti web o alcuni servizi risultassero necessari per lo svolgimento dell'attività aziendale, e impropriamente resi non disponibili, è possibile contattare i servizi assistenza facendo richiesta motivata al Servizio ICT (assistenza.rete@aosp.bo.it), e chiedendo l'abilitazione.

Il collegamento alla rete Internet è potenzialmente la sorgente principale di "infezione" della rete aziendale, intesa come lo scaricamento di dati e programmi (detti "malware") atti a minare l'integrità e funzionalità della rete interna o sottrarre dati. Per tale motivo è importante che ogni operatore/utente che abbia accesso alla rete Internet eviti di accedere a servizi non noti, o comunque estranei all'attività lavorativa, e mantenga un atteggiamento cauto nell'utilizzo di servizi esterni alla rete aziendale.

È obbligatorio inoltrare pronta segnalazione attraverso i canali di assistenza nel caso in cui, a seguito di navigazione sulla rete Internet o utilizzo di servizi esterni alla rete aziendale, dovessero manifestarsi comportamenti anomali della postazione di lavoro, o comunque qualora ci fosse il sospetto di tentativi di truffa/sottrazione dati/attacco informatico.

L'accesso alla rete Internet è monitorato, sia a tutela della sicurezza della rete aziendale, sia per prevenire eventuali usi impropri. Ogni altro controllo o intervento da parte del datore di lavoro sulla navigazione in Internet potrà avvenire esclusivamente in conformità alle finalità e ai limiti previsti dalla legge, dalla giurisprudenza o dall'Autorità Garante per la protezione dei dati personali.

6.6 Conservazione e tracciabilità

Nel rispetto dei principi cui all'art. 5 del GDPR "Principi applicabili al trattamento di dati personali" l'Azienda conserva per un periodo massimo di 6 mesi i log del sistema di posta elettronica e per un periodo di 3 mesi i log della navigazione Internet. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati entro i termini suddetti, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

Il contenuto dei file di log è così strutturato:

- mail: identificativo di autenticazione, indirizzo IP del PC, data e ora, mittente, destinatari, oggetto;
- Internet: identificativo di autenticazione, indirizzo IP del PC, data e ora, riferimento URL dei siti visitati.

I log vengono generati automaticamente dai sistemi sotto forma di file di testo.

Le attività di verifica e controllo sono svolte dal Servizio ICT esclusivamente per le seguenti finalità:

- motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware e software, ecc.);
- tutela del sistema informatico e/o del patrimonio informativo aziendale e degli strumenti informatici aziendali;
- sicurezza e verifica dell'efficacia delle misure di sicurezza adottate a protezione di dati, informazioni e infrastrutture.

Le attività di verifica e controllo sono svolte sugli strumenti e non sulle persone, e non sono mai svolte per finalità di controllo dell'attività lavorativa.

Le attività di verifica e controllo sopra descritte svolte dall'Azienda possono essere di due tipi:

a) **di routine**: eseguiti con periodicità sistematica dal Servizio ICT attraverso l'uso di strumenti specificatamente predisposti ed appositamente parametrati, ed hanno come scopo quello di consentire l'ordinaria gestione e manutenzione tecnica dei sistemi con la finalità di garantirne il corretto funzionamento;

b) **occasionali e puntuali**: sono quelli svolti occasionalmente a fronte di specifici eventi e circostanze atte, anche potenzialmente, a compromettere il funzionamento, la sicurezza e l'integrità del sistema informativo e del patrimonio aziendale. Tali controlli sono sempre condotti nel modo meno invasivo possibile, limitatamente alle sole aree del sistema interessate dagli eventi che generano la verifica, non prolungate nel tempo e limitate al periodo strettamente necessario ad assicurare funzionalità e sicurezza dei sistemi. I controlli di tipo occasionale e puntuale sono svolti dal Servizio ICT su autorizzazione della Direzione Generale, esclusivamente nei seguenti casi:

1) per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;

2) nel caso in cui si verifichi un evento dannoso o una situazione di particolare gravità che richiede un intervento immediato a fronte della possibile compromissione dei sistemi.

In ogni caso, eventuali controlli occasionali e puntuali, saranno svolti nel rispetto delle modalità di seguito descritte:

a) controllo preliminare dei dati (ad es. log) in forma anonima e aggregata riferiti all'intero sistema informatico e all'intera organizzazione lavorativa;
b) se necessario invio di un avviso collettivo/generalizzato contenente la segnalazione di un rilevato incidente, utilizzo anomalo, di un abuso o di un comportamento non conforme al presente Documento, accompagnato dall'avvertimento che, in caso di reiterazione, il Servizio ICT potrà procedere ad una verifica anche a carico di singole e specifiche aree o dei singoli strumenti informatici aziendali;
c) nel caso in cui le anomalie o gli abusi rilevati persistano o generino problemi o incidenti successivi, il Servizio ICT procede all'invio di un avviso destinato solo ad un'area determinata o a un singolo utente, ed al conseguente controllo/verifica eventualmente anche a carico di singole e specifiche aree o delle singole utenze o strumenti informatici aziendali.

La conservazione dei log risponde quindi alle seguenti finalità:

1. **gestione dei sistemi**:
- verifica e gestione a seguito di attacchi informatici (malware, phishing, ecc.);
- verifica e ottimizzazione dell'efficacia dei sistemi di protezione (antispam, web filtering, antivirus, ecc.);
- riscontro a segnalazione da parte degli utenti (perdita messaggi e-mail, mancata raggiungibilità di siti web, ecc.);
2. **statistiche di utilizzo**;
3. **eventuali controlli del datore di lavoro** che si rendessero necessari in circostanze eccezionali (ad es. per difendere propri diritti o interessi legittimi). L'Azienda non effettuerà, ad ogni modo controlli sui contenuti dei messaggi e-mail o sui contenuti dei siti visitati durante la navigazione.
4. **richieste da parte della Polizia Postale e/o dell'Autorità Giudiziaria**;
5. **esercizio dei diritti dell'interessato/utente previsti dagli artt. 15- 22 del Documento (EU) 2016/679**.

I log sono accessibili per la consultazione ed elaborazione ai soli Amministratori di Sistema appositamente nominati. Dopo il tempo di ritenuta (6 mesi per i log della posta elettronica e 3 mesi per i log della navigazione Internet) i dati saranno eliminati in maniera definitiva.

6.7 Responsabilità conseguenti alla violazione di quanto definito nel documento

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente documento.

Il mancato rispetto o la violazione delle regole di cui al presente documento da parte del personale dipendente, a prescindere dalle misure di tipo preventivo eventualmente applicabili ed applicate, è in ogni caso perseguibile con i provvedimenti disciplinari previsti dal vigente CCNL applicabile all'utente che ha commesso la violazione, nonché con tutte le azioni, anche di tipo risarcitorio, in ambito civile, penale ed amministrativo.

Nei confronti del personale non dipendente autorizzato a prestare la propria attività lavorativa all'interno dell'Azienda, o comunque autorizzato al trattamento dei dati, in caso di violazioni del seguente documento, saranno applicabili le misure preventive della revoca dell'assegnazione e/o dell'autorizzazione all'uso degli strumenti informatici aziendali e della rete informatica aziendale e la sospensione, interruzione e/o risoluzione del rapporto contrattuale in corso, nonché, in presenza dei necessari presupposti, il ricorso alle azioni amministrative e/o giudiziarie, anche di tipo risarcitorio, necessarie ai fini della tutela dei diritti e degli interessi dell'Azienda.

6.8 Attività di vigilanza

Oltre a quanto previsto nelle disposizioni precedenti del presente Documento, il personale incaricato del Servizio ICT effettuerà controlli anonimi, tramite l'analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e la rilevazione della tipologia di utilizzo (e-mail, file audio e video, file archiviati su server centrale, ecc.). Deve, infatti, per quanto possibile, essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Ove sia rilevata un'anomalia di funzionamento e/o di utilizzo degli strumenti informatici (ad es. picchi ingiustificati dell'attività di traffico di rete generato dalle postazioni di lavoro, anche verso internet; attività insolita per frequenza e per numerosità di messaggi e-mail inviati e/o ricevuti dall'account aziendale, anche attraverso l'utilizzo di mailing list o invii massivi; in generale l'adozione di comportamenti e/o abusi anche reiterati che possano compromettere il funzionamento dei sistemi aziendali) o nel caso di una situazione di rischio per la sicurezza del sistema informativo ospedaliero, il Servizio ICT può inviare via email un avviso generalizzato agli utenti dell'area o del settore interessati, evidenziando l'utilizzo irregolare degli strumenti aziendali e invitando gli utenti ad attenersi scrupolosamente alle disposizioni impartite.

Nel caso in cui la situazione di rischio o l'anomalia nell'utilizzo degli strumenti aziendali non sia risolvibile da un controllo su dati aggregati come sopra precisato, l'amministratore di sistema specificamente autorizzato per iscritto, anche con delega

generale, può effettuare controlli circoscritti su singole postazioni di lavoro, in conformità alle norme dell'ordinamento o alla giurisprudenza.

L'attività effettivamente eseguita sulla postazione di lavoro deve essere in ogni caso comunicata all'utente interessato senza ingiustificato ritardo al termine dell'intervento. Il Servizio ICT dovrà annotare, anche in modalità telematica, gli interventi svolti, specificando i motivi, la data e l'orario dell'intervento, dando atto degli avvisi intervenuti nei confronti del soggetto o dei soggetti interessati. In caso di contestazioni disciplinare, gli esiti dell'attività effettuata, saranno oggetto di confronto con l'interessato e, su richiesta dello stesso, con un rappresentante dallo stesso indicato.

6.9 Disposizioni finali

Il presente documento non esaurisce le misure di sicurezza aziendali: a tale proposito è necessario altresì osservare quanto disposto dal vigente documento Istruzione Operativa Aziendale in materia di protezione dei dati personali (IOA29), reperibile sul sito internet aziendale, alla sezione "La privacy in Azienda" (https://intranet.aosp.bo.it/files/ioa29_rev._7_del_11.06.2019.pdf.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte verranno esaminate dai Servizi aziendali competenti, a cadenza biennale.

7.0 ALLEGATI E MODULI UTILIZZABILI

R01/IOA99 Richiesta creazione casella PEC aziendale

T01/IOA99 Informativa sul trattamento dei dati personali agli utenti che utilizzano strumenti informatici aziendali