REGOLAMENTO GESTIONE PRIVACY E TRATTAMENTO DATI

Ai sensi dell'art. 29 del Regolamento generale sulla protezione dei dati personali n. 2016/679 (UE)

1 PRINCIPI GENERALI

Il presente documento ha l'obiettivo di assicurare le misure di sicurezza nella gestione del trattamento dei dati personali. Si fissano inoltre le linee guida cui debbono attenersi gli incaricati al trattamento dei dati e viene altresì regolamentato l'utilizzo di internet e posta elettronica per gli utenti di tali servizi nell'ambito della struttura di Fondazione A.S.F.A.P.

Questo documento è adottato da Fondazione A.S.F.A.P. su proposta del Responsabile della protezione dei dati personali e del Titolare dei dati personali, in conformità al Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR).

A tal proposito, allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che le principali fonti normative in materia sono le seguenti:
15 dicembre 2015 - Il Parlamento e il Consiglio raggiungono l'accordo, il testo è definitivo dopo la firma del gennaio 2016
8 aprile 2016 - Il Consiglio dell'Unione europea adotta il GDPR
12 aprile 2016 - La Commissione LIBE del Parlamento europeo approva il GDPR che quindi passa in plenaria
16 aprile 2016 - Il Parlamento europeo adotta il GDPR
4 Maggio 2016 - Pubblicazione del GDPR nella Gazzetta Ufficiale dell'UE
24 maggio 2016 - Il GDPR entra in vigore 20 giorni dopo la pubblicazione nella Gazzetta ufficiale dell'Unione europea
13 dicembre 2016 - Il Gruppo Articolo 20 adotta le linee guida per alcuni aspetti del GDPR

Copia del presente Regolamento viene pubblicata sul sito internet nella sezione "Regolamento Privacy" e consegnata a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività. L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'incaricato e per Fondazione A.S.F.A.P per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

2 CAMPO DI APPLICAZIONE

Le presenti Istruzioni si applicano:

- a tutti i lavoratori dipendenti e a tutti i collaboratori di Fondazione A.S.F.A.P a prescindere dal rapporto contrattuale con la stessa intrattenuto che si trovano ad operare sui dati personali di cui la Fondazione A.S.F.A.P. stessa è Titolare (di seguito "utenti");

- a tutte le attività o comportamenti comunque connessi al trattamento dei dati e all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

3 RIFERIMENTI NORMATIVI E DEFINIZIONI

Gli Incaricati sono le persone fisiche autorizzate a compiere le operazioni di trattamento dei dati dal Titolare o dal Responsabile (art. 4 n. 10 GDPR). La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si evidenzia preliminarmente che, ai fini del presente documento:

• con il termine "trattamento" (art. 4, comma 1, lett. a) ci si riferisce ad una qualunque operazione effettuata sui dati, svolta con o senza l'ausilio di mezzi automatizzati, che abbia come oggetto la raccolta, la registrazione, la consultazione, l'elaborazione, la modifica, la diffusione, l'estrazione, la distruzione di dati, anche se non registrati in una banca dati; il trattamento comprende l'intera vita del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine; di conseguenza, si parla di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano;

• con il termine "dato personale" (art. 4 N.1 GDPR) si intende qualsiasi informazione (es. nome) concernente una persona fisica identificata o identificabile, anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari (Convenzione 108, art. 2, lett. a) e Direttiva sulla protezione dei dati, articolo. 2, lett. a). La persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato".

• con il termine dati soggetti a trattamento speciale (ex dati sensibili) si fa riferimento ai dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato;

• con il termine "dato giudiziario" si fa riferimento ai dati idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di procedura penale.

4 LINEE GUIDA

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.
Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

• tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

• le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

• in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

• non devono essere eseguite operazioni di trattamento per scopi non previsti dalle finalità del trattamento;

• devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;

• deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.
Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

4.1 ACCESSO AI DATI TRAMITE PC

La postazione di lavoro deve essere:

• utilizzata solo per scopi legati alla propria attività lavorativa;

• utilizzata in modo esclusivo da un solo utente;

• protetta, evitando che terzi possano accedere ai dati che si sta trattando.

Occorre, inoltre, precisare che è dovere dell'Incaricato:

• non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, ecc.);

• richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo max.5 minuti di inattività;

• non lasciare incustoditi cellulari e tablet;

• non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

4.2 GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun Incaricato deve aver cura di:

• modificare, alla prima connessione, quella che L'Amministratore di rete ha attribuito di default;

• cambiarla almeno ogni 90 giorni, o immediatamente nei casi in cui sia compromessa;

• comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;

• usare sia lettere che numeri e almeno un carattere maiuscolo;

• non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.,

• mantenerla riservata e non divulgarla a terzi;

• non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;

• non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;

• non comunicarla mai per telefono salvo gravi necessità;

4.3 ANTIVIRUS

I Personal Computer (PC) di Fondazione A.S.F.A.P., pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti. Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

• controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;

• chiudere correttamente i programmi in uso;

• non aprire, se si lavora in rete, file sospetti e di dubbia provenienza;

• non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate;

• verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati prima dell'esecuzione dei file in esso contenuti;

• non utilizzare CD-Rom o altri supporti elettronici di provenienza incerta;

• porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;

• usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;

• non modificare le configurazioni impostate sul proprio PC;

• spegnere il PC al termine dell'utilizzo;

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'Incaricato:

a. sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto;

b. contatti immediatamente l'Amministratore di rete;

c. chiuda il sistema e le relative applicazioni.

4.4 SALVATAGGIO DEI DATI

Tutti i dati al termine della giornata lavorativa verranno salvati sul server di Fondazione A.S.F.A.P. A tale riguardo, qualora vi sia la necessità, l'Incaricato può richiedere all'Amministratore di rete la creazione sul server di una cartella a lui intestata o, in alternativa, di una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Incaricato stesso.

4.5 PROTEZIONE DEI PC PORTATILI

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.
Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

• conservare lo strumento in un luogo sicuro al temine del lavoro;

• non lasciare mai incustodito il PC in caso di utilizzo in ambito esterno all'azienda;

• avvertire tempestivamente l'Amministratore di rete, che darà le opportune indicazioni, in caso di furto di un PC portatile;

• operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

4.6 INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno a Fondazione A.S.F.A.P.
In particolare, l'utente dovrà osservare le seguenti regole:

• è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento del proprio incarico;

• non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;

• non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;

• non è consentito l'utilizzo funzioni di instant messaging a meno che autorizzate dall' Amministratore di rete;

• è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto o oggetto non chiaro);

• è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;

• occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;

• occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina di virus e altri elementi potenzialmente dannosi;

• è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete (creando così un collegamento tra la rete aziendale interna e la rete esterna);

• al fine di ottimizzare le risorse a disposizione della posta elettronica e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.

• va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente l'Amministratore di rete nel caso in cui siano rilevati virus.

• utilizzare esclusivamente supporti di origine esterna che possano essere criptati anche se sono da preferire strumenti di archiviazione in cloud (Dropbox, Google drive, OneDrive ecc..)

4.6.1 Particolari cautele nella predisposizione dei messaggi di posta elettronica.

Nell'utilizzo della posta elettronica ciascun utente deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto, si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione di ondazione A.S.F.A.P.

Fondazione A.S.F.A.P. formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dagli enti pubblici;

b) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:
- visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,
- una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,
- cancellare il messaggio e svuotare il "cestino" della posta,
- segnalare l'accaduto all'Amministratore di rete.

c) evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta:
in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;

d) in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica:

- adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,
- utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi,
- in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.

e) in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;

f) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

4.7 TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati trattati da Fondazione A.S.F.A.P. da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali. Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

• prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

• verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;

• nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;

• in caso di trasmissione di dati sensibili è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata. Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

Si ricorda che, in base all' art. 9 del GDPR, il trattamento dei dati sensibili può essere effettuato solo con l'esplicito consenso da parte dell'interessato.

4.8 ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro. L'accesso a tutti i locali di Fondazione A.S.F.A.P. deve essere consentito solo a personale autorizzato.

5 ACCESSO AI DATI DELL'UTENTE

L'Amministratore di rete può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Lo stesso Amministratore di rete può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).
L'Amministratore di rete, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica dell'utente per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'utente. L'Amministratore di rete può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario

svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. L'eventuale controllo sui file di log da parte dell'Amministratore di rete ma non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.
Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico. L'Amministratore di rete è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc. Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti. In ogni caso, Fondazione A.S.F.A.P. garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

• lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

• riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

• lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

6 CONTROLLI DA PARTE DI FONDAZIONE A.S.F.A.P.

Con il presente capitolo portiamo all'attenzione degli incaricati la possibilità di Fondazione A.S.F.A.P. di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.
A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà di Fondazione A.S.F.A.P in quanto mezzo di lavoro.
È pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli di Fondazione A.S.F.A.P.
Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati da Fondazione A.S.F.A.P. nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento. In caso di anomalie, Fondazione A.S.F.A.P., per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia. In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. In caso di successive, perduranti anomalie, ovvero ravvisandone

la necessità, Fondazione A.S.F.A.P. si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

7 RESPONSABILITÀ E SANZIONI

L'utente, al fine di non esporre sé stesso e Fondazione A.S.F.A.P. a rischi sanzionatori sia amministrativi che penali, è tenuto a adottare comportamenti puntualmente conformi alla normativa vigente in materia di protezione dei dati (Regolamento generale per la protezione dei dati personali n. 2016/679) ed alla regolamentazione di Fondazione A.S.F.A.P.

Il presente Documento è stato predisposto dal Responsabile per la Protezione dei dati ed approvato dal Titolare del Trattamento dei dati.

Como, 17 gennaio 2020

Il Titolare del Trattamento dati

_____

Il Responsabile della Protezione dei dati

_____