Dal 1958
tappezzieri in stoffa

Policy in materia di Protezione e Trattamento dei Dati Personali

Villa Tappezzieri

24 maggio 2018

Versione Policy in materia di protezione dei dati personali (Protection of Personal Information, PPI) [001.V1.IT]

Storico delle versioni: 1.0

1. INTRODUZIONE

Scopo

Il presente documento riassume le procedure ed i principi adottati da Villa Tappezzieri in materia di tutela della Privacy e in particolare in relazione al trattamento dei dati personali ("Dati") comunicati od acquisiti da Villa Tappezzieri nell'esecuzione delle proprie attività aziendali.

I Dati saranno sempre trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Sulla base dell'analisi dei rischi effettuata da tecnici e consulenti esterni, nel presente documento sono riassunti:

- *i criteri e le procedure per garantire la sicurezza nel trattamento dei dati personali;*
- *la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:*
- *i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;*
- *i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati;*
- *i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;*
- *i criteri e le procedure per il ripristino dell'accesso ai dati;*
- *l'elaborazione di un piano di formazione per rendere edotti i responsabili del trattamento dei rischi individuati e dei modi per prevenire gli eventuali danni.*

L'efficacia di tali misure di sicurezza sarà oggetto di controlli continuativi e audit periodici, da eseguirsi almeno con cadenza annuale.

Ambito e applicabilità

La presente Policy riguarda tutti i Dati personali raccolti, elaborati, condivisi o usati da Villa Tappezzieri. Si applica a tutti i dipendenti, collaboratori e consulenti. La presente Policy entra in vigore il 24/05/2018.

Copia della presente Policy viene pubblicata sul sito internet di Villa Tappezzieri (www.villatappezzieri.it) nella sezione "Privacy Policy" e consegnata a ciascun dipendente, collaboratore e consulente in forma cartacea o digitale.

Le prescrizioni descritte nel presente documento si applicano a tutti i trattamenti eseguiti nell'ambito dell'intera struttura organizzativa di Villa Tappezzieri, dagli eventuali Responsabili e da tutti gli incaricati, e sono da considerarsi vincolanti nei rapporti contrattuali relativi a trattamenti eseguiti da altri soggetti esterni cui sia conferito un incarico di Responsabile del trattamento di dati di cui Villa Tappezzieri sia Titolare.

2. DEFINIZIONI

Nel presente documento:

- *con il termine "trattamento" (art. 4, n. 2, del Regolamento UE 2016/679) ci si riferisce ad una qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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;*
- *con il termine "dato personale" (art. 4, n. 1, del Regolamento UE 2016/679) si fa riferimento a 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;

- *con il termine "profilazione" (art. 4, n. 4, del Regolamento UE 2016/679) si fa riferimento a qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;*
- *con il termine "pseudonimizzazione" (art. 4, n. 5, del Regolamento UE 2016/679) si fa riferimento al trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*
- *con il termine "titolare del trattamento" (art. 4, n. 7, del Regolamento UE 2016/679) si fa riferimento alla persona fisica o giuridica, all'autorità pubblica, al servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;*
- *con il termine "responsabile del trattamento" (art. 4, n. 8, del Regolamento UE 2016/679) si fa riferimento alla persona fisica o giuridica, all'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.*

3. FUNZIONI ORGANIZZATIVE RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI

Titolare del trattamento

Il Titolare del trattamento, nella figura del legale rappresentante di Villa Tappezzieri, avvalendosi ove necessario dei Responsabili del trattamento (art. 28 del Regolamento UE 2016/679), ove nominati:

- *individua e prende decisioni in ordine alle finalità ed alle modalità di trattamento dei dati, ivi compreso il profilo della sicurezza;*
- *effettua il censimento ed aggiorna il registro delle attività di trattamento dei dati e garantisce all'interessato tutti i diritti di cui agli artt.15-21 del Regolamento UE 2016/679;*
- *individua, predispone, verifica, documenta e rende note le misure di sicurezza (minime e più ampie) necessarie per la protezione dei dati personali.*

Responsabili del trattamento

Ove nominati, i Responsabili del trattamento gestiscono i trattamenti sulla base dei compiti affidati e analiticamente specificati per iscritto dal Titolare. I Responsabili si attengono alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento previste dal Regolamento, ivi compreso il profilo relativo alla sicurezza. I Responsabili per il trattamento vigilano sul rispetto delle istruzioni impartite agli incaricati al trattamento.

Trattamento sotto l'autorità del Titolare o del Responsabile

A ciascun dipendente assegnato, all'atto dell'assunzione o nel caso di cambiamento di mansione, presso un'unità organizzativa ove sono trattati i dati, sono state fornite istruzioni per operare, nell'ambito dei trattamenti assegnati, con la massima diligenza ed attenzione e rispettando le misure di sicurezza predisposte da Villa Tappezzieri.

4. LINEE GUIDA PER DIPENDENTI, COLLABORATORI E CONSULENTI

Di seguito vengono descritte le norme alle quali i dipendenti e/o i consulenti devono attenersi nell'esecuzione dei compiti che implicano un trattamento di Dati personali.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei Dati personali oggetto del trattamento, i dipendenti, i collaboratori e/o i consulenti devono 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;*
- *nell'ipotesi in cui un soggetto interessato revochi il proprio consenso al trattamento dei dati ex art. 7, comma 3, del Regolamento, il dipendente e/o consulente è tenuto a darne tempestiva comunicazione al Titolare o, se presente, al Responsabile per l'adozione di ogni necessario provvedimento del caso;*
- *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;*
- *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.*

Accesso ai dati dalla postazione/strumento di lavoro

La postazione e gli strumenti di lavoro devono essere:

- *utilizzati solo per scopi legati alla propria attività lavorativa;*
- *utilizzati in modo esclusivo da un solo utente;*
- *protetti, evitando che terzi possano accedere ai dati che si stanno trattando.*

Occorre, inoltre, precisare che è dovere di ciascun dipendente, collaboratore e/o consulente:

- *non installare alcun software e/o applicazioni mobile non preventivamente autorizzato;*
- *non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, periferiche, ecc.);*
- *richiamare le funzioni di sicurezza del sistema operativo (sequenza dei tasti CTRL+ALT+CANC per i sistemi Windows e attivazione della funzione Lock Workstation per i sistemi Windows e sequenza ⌘-control-Q per i sistemi Mac) in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo massimo 5 minuti di inattività;*
- *non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);*
- *non lasciare incustoditi smartphone;*
- *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.*

Lo smartphone dato in dotazione al dipendente, collaboratore o consulente è dotato di un codice di blocco che viene verificato una volta all'anno.

Gestione delle password

Per una corretta gestione delle password, ciascun dipendente, collaboratore e/o consulente deve aver cura di:

- *modificare, alla prima connessione, quella che l'Area IT 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.*

Antivirus

Le attrezzature hardware in dotazione ai dipendenti, collaboratori e consulenti (personal computer desktop o laptop, tablet e smartphone) 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 non è cura del dipendente, ma di Villa Tappezzieri;*
- *chiudere correttamente i programmi in uso;*
- *non aprire, se si lavora in rete, files sospetti e di dubbia provenienza;*
- *non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate;*
- *non sottoscrivere abbonamenti sia gratuiti che a pagamento con servizi in Cloud che non siano state preventivamente approvate e autorizzate;*
- *verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati (CD-Rom o USB), prima dell''esecuzione dei file in esso contenuti;*
- *non utilizzare CD-Rom, USB o altri supporti elettronici di provenienza incerta;*
- *porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC, dandone comunicazione all'Area IT;*
- *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 della giornata di lavoro.*

Alla verifica di un malfunzionamento del PC o dello smartphone, che può far sospettare la presenza di un virus, è bene che il dipendente, collaboratore e/o consulente:

a) sospenda ogni operazione sul PC/smartphone evitando di lavorare con il sistema infetto;
b) contatti immediatamente l'Area IT;
c) chiuda il sistema e le relative applicazioni.

Protezione di pc portatili, smartphone e tablet

Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili (pc portatili, tablet e smartphone):

- *conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;*
- *non lasciare mai incustodito il pc o il smartphone in caso di utilizzo in ambito esterno all'azienda;*
- *avvertire tempestivamente l'Area IT, che darà le opportune indicazioni, in caso di furto di un PC portatile o di uno smartphone;*
- *essere sempre ben consapevole delle informazioni archiviate sul portatile o sul smartphone che sono maggiormente soggetti a furto e smarrimento rispetto alla postazione fissa;*
- *operare sempre nella massima riservatezza quando si utilizza il PC portatile o il smartphone in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.*

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 Villa Tappezzieri.

In particolare, l'utente dovrà osservare le seguenti regole:

- *è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;*
- *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;*
- *le uniche funzioni di Instant Messaging consentite sono quelle comunicate dall'Area IT;*
- *è assolutamente vietato accedere alla posta elettronica da sorgenti diverse da quelle aziendali;*
- *è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);*
- *non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;*
- *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 (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;*
- *è consentito solo l'utilizzo dei programmi installati dall'Area IT;*
- *è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate da Villa Tappezzieri;*
- *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 aziendale 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 aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);*
- *al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale 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 prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.).*

Reti Wi-Fi / LAN

Gli apparati potranno essere collegati alla rete Wi-Fi aziendale durante la permanenza in ufficio. In situazioni diverse il dipendente, collaboratore e/o consulente potrà decidere di collegarsi a una rete wi-fi diversa se ritenuta sicura e attendibile.

L'accesso alle reti Villa Tappezzieri è consentito esclusivamente a dipendenti, collaboratori e consulenti, che hanno ricevuto le relative credenziali di accesso dall'Area IT.

5. CENSIMENTO DEI TRATTAMENTI ED ANALISI DEI RISCHI

Villa Tappezzieri ha effettuato ed effettuerà periodicamente il censimento e l'analisi dei rischi secondo la best practice di settore.
Vedi:
- *Tabella 2.1 DPS del 22/05/2018*
- *Registro dei Trattamenti del 24 maggio 2018*

6. MISURE DI SICUREZZA IN ESSERE

Al fine di assicurare l'integrità dei dati trattati e impedirne la comunicazione e/o diffusione non autorizzata, Villa Tappezzieri ha adottato misure di sicurezza di tipo fisico (relativamente alla conservazione dei dati su supporto cartaceo) ed informatico.

Villa Tappezzieri si è dotata delle misure di protezione minime, previste e descritte nel DPS.

Gli armadi e le cassettiere presenti negli uffici e nei quali vengono archiviati i documenti con dati riservati sono chiusi a chiave; la chiave è conservata dal dipendente che gestisce i documenti stessi. L'ingresso agli uffici è possibile previa disattivazione dell'allarme – attraverso apposita chiavetta – e apertura della serratura.

7. FORMAZIONE

Con cadenza almeno annuale sono organizzati incontri o viene reso disponibile materiale formativo per il personale del Villa Tappezzieri relativamente alle norme in materia di tutela della Privacy.

8. VIOLAZIONE DEI DATI

Ciascun dipendente e/o consulente è tenuto a comunicare tempestivamente, e comunque non oltre 24 ore o 2 ore lavorative dal momento in cui ne è venuto a conoscenza, di ogni violazione della sicurezza dei Dati personali e/o di ogni altro evento che possa comunque comprometterne la sicurezza, così da consentire al Titolare e/o, ove presente, al Responsabile di ottemperare alle previsioni di cui agli artt. 33 e 34 del Regolamento.

***