REGOLAMENTO PER LE PROCEDURE DI ACCESSO AGLI ARCHIVI NEL RISPETTO DELLE NORME IN MATERIA DI TRATTAMENTO DEI DATI.

Via Favetti 7, 33080 CASTIONS di Zoppola (Pn)
C.F. e P.IVA 00221260938
Amministrazione Tel. 0434/97187
Scuola Favetti 0434/317731 – Infermeria 0434/97016
Mail: fondazione@micolitoscano.it
Pec: fondazione@pecfvg.it

La Fondazione Micoli-Toscano adotta ufficialmente il contenuto del seguente documento come da delibera del 30 maggio 2023: *"il Consiglio prende atto della formazione, dell'adozione e dell'aggiornamento, ai fini dell'approvazione, dei documenti che […] definiscono e regolamentano le procedure di accesso agli archivi nel rispetto delle norme in materia di trattamento dei dati;*

Al momento dell'assunzione o in fase successiva (ad es. per cambio mansioni), i dipendenti che trattano dati personali sottoscrivono il modulo GDPR M01 "nomina autorizzati al trattamento".

All'interno del suddetto documento GDPR M01 vengono indicati i trattamenti autorizzati per ogni dipendente, secondo la propria mansione.

Oltre alla consegna del suddetto modello, i dipendenti trovano riferimenti o ulteriori procedure nel "fascicolo informativo autorizzati al trattamento", qui allegato.

La raccolta ed archiviazione dei dati cartacei avviene in appositi armadi-archivio, chiusi con chiave, dei quali è indicato il contenuto con apposita targhetta esterna, di modo che ne sia riservato l'accesso esclusivamente all'incaricato del trattamento.

Analogamente i dati informatici sono raccolti in cartelle residenti sul server, il cui accesso è regolamentato da apposita autorizzazione attuata dal Responsabile dei sistemi informativi, su indicazione della Direzione. Nella "Relazione tecnica sui sistemi informatici" qui allegata, si evidenzia la consistenza della rete informatica e le relative caratteristiche.

Allegati:

- Allegato 1_FASCIOLO INFORMATIVO IN MATERIA DI TRATTAMENTO DATI PERSONALI
- Allegato 2_ Relazione tecnica sui sistemi informatici

Allegato 1

FASCICOLO INFORMATIVO IN MATERIA DI TRATTAMENTO DATI PERSONALI

per addetti o collaboratori di Fondazione Micoli-Toscano

INDICE

Via Favetti 7, 33080 CASTIONS di Zoppola (Pn)
C.F. e P.IVA 00221260938
Amministrazione Tel. 0434/97187
Scuola Favetti 0434/317731 – Infermeria 0434/97016
Mail: fondazione@micolitoscano.it
Pec: fondazione@pecfvg.it

ALCUNE DEFINIZIONI UTILI PRIMA DI INIZIARE

INTERESSATO: indica la persona fisica (ivi comprese le ditte individuali e i liberi professionisti) a cui i dati personali si riferiscono.

TRATTAMENTO: indica 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.

TITOLARE DEL TRATTAMENTO: indica il soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Il Titolare del trattamento nel nostro caso è FONDAZIONE MICOLI-TOSCANO nella persona del legale rappresentante.

RESPONSABILE DEL TRATTAMENTO: indica il soggetto (società o individuo) che tratta i dati personali per conto del titolare del trattamento.

La categoria dei responsabili esterni del trattamento comprende, tra gli altri, i fornitori di infrastrutture IT e chiunque tratta dati personali dei clienti (dipendenti e fornitori) di Udinese Calcio S.p.A. per conto della stessa.

I responsabili del trattamento di Fondazione Micoli-Toscano sono il consulente del lavoro, l'azienda che fornisce l'assistenza informatica, la società che si occupa della sicurezza e salute dei lavoratori, ecc.

DATA PROTECTION OFFICER (DPO): è una figura nuova che ha un ruolo di consulenza e vigilanza in azienda in materia di dati personali8.

Il DPO è individuato nella società Pratika S.r.l., e nella persona referente di Ilaria Galante (ilaria.galante@gruppopk.com).

VIOLAZIONE DEI DATI PERSONALI O *DATA BREACH*: indica 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.

COS'È UN DATO PERSONALE?

In pratica tutte le informazioni relative a un individuo e connesse alla sua vita sia professionale che privata. Si va dai nomi alle fotografie, dall'indirizzo e-mail ai dettagli bancari fino all'indirizzo IP.

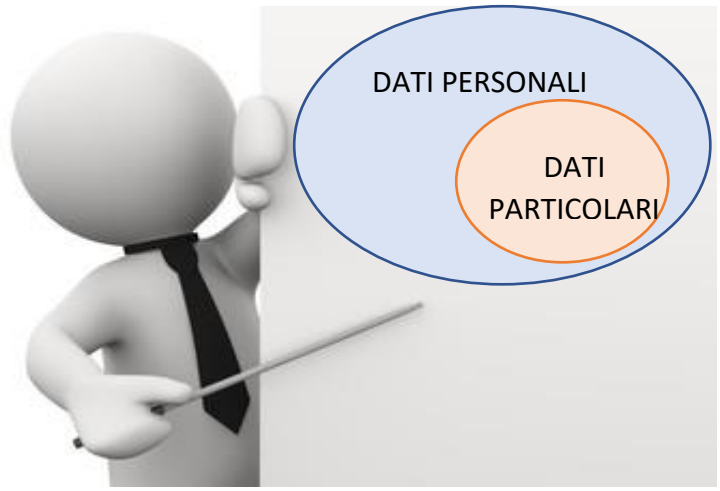
Si considerano dati personali tutti i dati che possono servire a identificare un individuo (quindi non una società, un'azienda!).

Alcuni dati aziendali potrebbero anche essere dati personali. mario.rossi@fiat.com è un dato personale in quanto l'indirizzo e-mail può essere ricollegato a una persona fisica e identificabile. Indirizzi e-mail come info@shift.it non sono invece considerati dati personali.

Una sottocategoria di dati personali sono i **DATI PARTICOLARI**, quelli che la vecchia normativa chiamava dati sensibili.

Particolari categorie di dati sono quelle che rivelano:

- Origine razziale ed etnica
- Opinioni politiche
- Convenzioni religiose o filosofiche
- Appartenenza sindacale
- Dati genetici e/o biometrici
- Dati relativi alla salute
- Dati relativi alla vita o all'orientamento sessuale



COME VANNO TRATTATI I DATI PERSONALI?

Il GDPR, nell'intenzione dei legislatori europei, è ispirato a tre cardini fondamentali:

PRIVACY BY DEFAULT ovvero: ogni impresa è tenuta a tutelare la vita privata degli interessati "di default" e cioè dev'essere una scelta di base, cosciente, predefinita e continuativa nel tempo che l'impresa deve trattare come valore fondante nel suo operare.

PRIVACY BY DESIGN ovvero: la protezione dei dati degli interessati deve partire dalla progettazione di ogni processo aziendale, deve esser parte del disegno iniziale e non un "adeguamento" postumo.

ACCOUNTABILITY, lo si può tradurre come responsabilizzazione e rendicontazione. Vuol dire che il Titolare del trattamento, ossia UDINESE CALCIO SpA, deve essere affidabile, capace e competente nel gestire i dati personali in conformità alla normativa e deve saper "render conto a terzi delle scelte compiute".

Cosa vuol dire trattare i dati in maniera conforme?

• Il trattamento deve essere **lecito**, **corretto**, **trasparente**;	Vuol dire che il Titolare può trattare i dati solo in quando c'è una di queste condizioni: • presenza di **obbligo di legge** *(es. normativa fiscale che mi impone di fare la fattura)* • per adempimento di **obblighi contrattuali** *(es. rapporto di lavoro)* • per tutelare **interessi vitali** *(di fatto non interessa Udinese)* • per un **interesse legittimo** prevalente del Titolare *(es. marketing su clienti già acquisiti)* • grazie all'ottenimento di un **consenso** (*solo quando non riesco a soddisfare nessuno degli altri punti es. utilizzo di foto di terzi)*
• I dati sono raccolti per **finalità determinate**, **esplicite** e **legittime**, e successivamente trattati in linea con tali finalità;	Vuol dire che il Titolare deve comunicare all'interessato per cosa tratterà i dati e dovrà nel tempo rispettare quanto comunicato
• I dati devono essere **adeguati**, **pertinenti** e **limitati** rispetto alle finalità (minimizzazione dei dati);	Vuol dire che il Titolare non può raccogliere più dati rispetto a quelli che effettivamente servono per le finalità che ha dichiarato
• Conservati per un **arco di tempo limitato** al conseguimento delle finalità (oltre questo tempo il dato va cancellato o reso anonimo);	Vuol dire che il Titolare non può conservare i dati per sempre. Ogni dato, in base alla finalità per cui è stato raccolto ha un tempo di vita prescritto per legge o deciso dal Titolare stesso

Per i dati particolari invece…

Il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una di queste (elenco non esaustivo: si indicano solo quelli interessanti ai nostri fini):

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è necessario per uno dei seguenti scopi:
  - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
  - per tutelare un interesse vitale dell'interessato o di un'altra persona fisica;
  - per accertare, esercitare o difendere un diritto in sede giudiziaria;
  - per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;

Nelle attività di FONDAZIONE MICOLI-TOSCANO va posta particolare attenzion

- **TRATTAMENTO DI DATI SANITARI**
- **EFFETTUAZIONE, UTILIZZO, DIFFUSIONE DI FOTO**

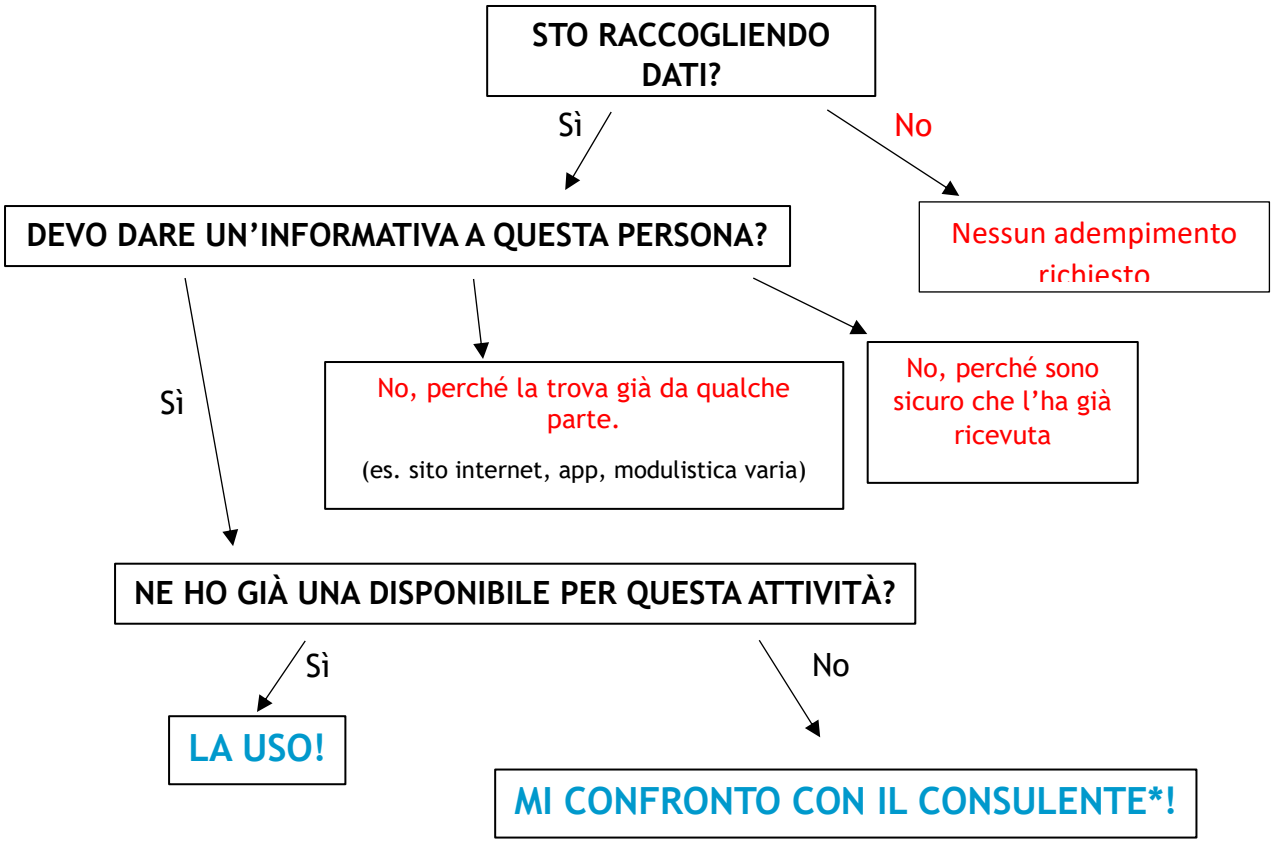
- Il trattamento di dati personali deve avvenire nel rispetto del **principio di riservatezza** della persona dell'interessato al trattamento e deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
- Il trattamento di dati personali deve inoltre avvenire nel rispetto della **dignità della persona** dell'interessato.
- Visite e medicazioni sono eseguite in una stanza idonea al fine di garantire all'ospite la dovuta privacy: gli interventi sul paziente avvengono in ambiente chiuso o almeno riparato dagli altri ospiti (con utilizzo di paravento) al quale può accedere solo il personale medico o infermieristico o di assistenza.
- Il personale **non può comunicare dati** riguardanti patologie e/o terapie in atto di un paziente tranne che al personale sanitario interessato alla sua cura o al famigliare di riferimento.
- La documentazione sanitaria dell'ospite, costituendo "documento ufficiale", **non può**, in originale, uscire dalla struttura tranne che per esplicita richiesta di un magistrato. Copia della stessa può essere al personale sanitario in caso di assoluta necessità a scopo di diagnosi e cura (ricovero ospedaliero).
- Nel visionare, elaborare, conservare, modificare, distruggere, comunicare dati personali su supporto cartaceo, gli incaricati sono tenuti alla **massima riservatezza**.
- Gli incaricati **non possono lasciare incustoditi ed esporre documenti** riportanti dati personali. A questo proposito, è fatto **divieto mostrare a terzi**, senza la preventiva autorizzazione del Titolare, **qualsiasi documento** conservato negli uffici riportante dati personali.

- I documenti e le cartelle contenenti dati sensibili o giudiziari sono custoditi, quando non utilizzati, sempre in stanze, **armadi o cassettiere dotati di serratura**.
- Le chiavi in grado di aprire le serrature sono affidate dal Titolare solo ed esclusivamente agli incaricati autorizzati ad accedere ai dati personali ivi contenuti. È vietato a tutti gli incaricati possessori di chiavi, lasciare queste incustodite e/o inserite nella serratura; è altrettanto vietato affidarle a soggetti non autorizzati al trattamento dei dati custoditi o, peggio ancora, ad esterni.
- È fatto **divieto** a tutti gli incaricati **effettuare copie o portare documenti fuori dai locali** delle strutture senza il preventivo consenso del Titolare e, per i dati sensibili, senza il consenso scritto dell'interessato.
- Nell'utilizzo dei software gestionali (Insoft, Genesys…) è necessario che ogni operatore faccia il **log-in con il proprio profilo e al termine dell'utilizzo effettui il log-out**, così da avere sempre certezza dell'attribuibilità delle operazioni.
- Il personale addetto all'animazione e alle attività che coinvolgono l'ospite deve essere reso edotto di eventuali negazioni di consenso su **effettuazione o utilizzo di foto** ritraenti la persona dell'ospite agendo di conseguenza. Di conseguenza, in base ai **consensi ottenuti**, l'attività di effettuazione e utilizzo foto dovrà essere coerente con essi.
- Il personale che effettua fotografie e riprese video, nell'effettuarle e in particolar modo in un eventuale utilizzo successivo deve sempre tenere in considerazione che deve essere rispettata costantemente la **dignità dell'ospite** ritratto.
- Il personale è tenuto a **comunicare immediatamente, e comunque senza ingiustificato ritardo, eventuali situazioni che possano costituire potenziali violazione di dati personali**: perdita di documentazione; cancellazione (anche accidentale) di file e altre informazioni; comunicazione a terzi di notizie e informazioni che non erano titolati a conoscere; apertura di file di dubbia provenienza e di allegati di mail dubbi… La valutazione dell'evento spetterà poi all'Ente.

DIRITTO A ESSERE INFORMATO

L'informativa va consegnata all'interessato ogni qualvolta vi sia un trattamento di dati. L'obbligo di informare gli interessati va adempiuto prima procedere, o al massimo al momento in cui si dà avvio alla raccolta dei dati. Non sussiste, invece, obbligo di fornire l'informativa se il trattamento riguarda dati anonimi (es. aggregati).

Per sapere se l'attività che sto facendo richiede la gestione di un'informativa questo di seguito illustrato è il ragionamento.



*scrivere a: ilaria.galante@gruppopk.com

ALTRI DIRITTI DELL'INTERESSATO

OPPOSIZIONE	L'interessato può opporsi al trattamento dei dati che lo riguardano solo se presenta motivi specifici a sostegno. Nel caso in cui i motivi siano validi, il Titolare non potrà più trattare i dati dall'interessato, a meno che non si dimostri che è necessario per motivi prevalenti.
INFORMAZIONE	L'interessato può richiedere al titolare informazioni che riguardino il trattamento dei suoi dati personali e il titolare è tenuto a fornire all'interessato tutte le informazioni richieste. Il titolare dovrà verificare l'identità del richiedente.
ACCESSO	L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni relative al trattamento.
LIMITAZIONE	L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato chiede quindi che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
CANCELLAZIONE (OBLIO)	L'interessato può chiedere al titolare del trattamento di tali dati la loro cancellazione e quest'ultimo deve procedere a ciò senza ingiustificato ritardo in tutti i casi in cui i dati personali non siano più necessari rispetto alle finalità per cui erano stati raccolti, oppure siano stati trattati illecitamente, oppure l'interessato revochi il consenso o si opponga al loro trattamento, oppure la cancellazione costituisca un obbligo giuridico imposto dal diritto dell'UE o degli Stati membri.
PORTABILITÀ	Consente a chiunque sappia che i suoi dati sono oggetto di trattamenti automatizzati, o col suo consenso o per contratto, di chiedere che i dati da lui forniti siano trasmessi a sé stesso o ad altro titolare da lui indicato, utilizzando un formato "strutturato, di uso comune e leggibile da dispositivo automatico".
RETTIFICA	L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

All'atto della ricezione, via mail o verbale, della richiesta di un interessato di esercitare un suo diritto relativamente alla protezione dei dati personali, è necessario inoltrare immediata comunicazione alla Direzione e al DPO, ed eventualmente al referente IT se il tipo di richiesta prevede un suo coinvolgimento.

Della gestione e soddisfazione della richiesta saranno poi gli uffici competenti ad occuparsene.

GESTIONE DELLE FIGURE CHE TRATTANO DATI

GESTIONE DELLE FIGURE INTERNE

La gran parte dei dipendenti di Fondazione Micoli-Toscano devono essere individuati quali "**autorizzati al trattamento**".

L'autorizzato al trattamento (o incaricato), è una persona fisica che materialmente svolge operazioni sui dati personali. L'autorizzato opera in subordinazione al titolare del trattamento. Il soggetto autorizzato deve ricevere adeguata formazione.

A ogni dipendente che tratta dati personali viene fatto sottoscrivere il modulo dedicato: si tratta di un incarico in cui a ciascun dipendente viene indicato a quali attività di trattamento viene autorizzato, in base alla propria mansione.

La lettura del presente fascicolo informativo è parte integrante della tua formazione come autorizzato!

GESTIONE DELLE FIGURE ESTERNE

È necessario poi disciplinare i rapporti con i fornitori che trattano dati per conto di Fondazione Micoli-Toscano. Questi fornitori si classificano come "**Responsabili del trattamento**" ex art. 28 GDPR.

Il Contratto di nomina verrà fornito a quei fornitori di servizi che, in forza del contratto trattano dati personali per conto dell'Ente (ovvero dati riferiti a dipendenti, collaboratori/fornitori, ospiti, utenti in genere).

Alcuni fornitori non saranno interessati da questi documenti perché il servizio che offrono non comporta alcun trattamento di dati personali.

Questi documenti sono declinati poi in modo specifico per determinate categorie di fornitori, come gli amministratori di sistema.

Nel caso di nuovi rapporti contrattuali con fornitori è necessario farsi queste domande ed eventualmente confrontarsi con i responsabili delle aree e con il DPO.

REGOLE IN MATERIA DI INFORMATION SECURITY

- non violare il segreto e la riservatezza delle informazioni trattate;
- proteggere i dati contro i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito;
- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- utilizzare soltanto per rendere la prestazione lavorativa gli eventuali strumenti tecnologici "aziendali", quali computer, smartphone, ecc., che il Titolare abbia concesso in uso anche al di fuori della struttura;

- contattare il Titolare o l'amministratore di sistema per qualsiasi dubbio, sospetto di incidente o di violazione che possa compromettere i dati aziendali o dello studio professionale.

UTILIZZO DI DISPOSITIVO PERSONALE PER ATTIVITÀ LAVORATIVE

Qualora il lavoratore utilizzi (= SIA AUTORIZZATO AD UTILIZZARE) un dispositivo personale per eseguire la prestazione lavorativa, deve aver cura di:

- utilizzare un dispositivo, se possibile, ad uso esclusivo personale (non cedendolo a altri);
- creare un account personale nel caso in cui il dispositivo sia ad uso condiviso con i familiari e in modo che il lavoratore acceda ad una partizione a suo uso esclusivo;
- proteggere l'accesso al dispositivo (o alla propria partizione) con credenziali conosciute soltanto del lavoratore, evitando qualsiasi forma di condivisione;
- evitare il ricorso a credenziali facilmente intuibili o ricostruibili;
- verificare che il dispositivo sia aggiornato quanto a misure di protezione, quali antivirus, antimalware, e firewall (a tal fine il Datore di lavoro indicherà i tool di sicurezza più adatti);
- verificare che il dispositivo sia aggiornato con l'ultima versione disponibile del sistema operativo su cui gira;
- non salvare i "documenti aziendali" nella memoria del proprio dispositivo o in altre periferiche personali laddove siano disponibili funzioni di salvataggio su server aziendali;
- non aprire allegati o link che destino sospetti;
- non scaricare programmi di dubbia provenienza;
- disconnettersi accuratamente a fine sessione dagli applicativi aziendali.

UTILIZZO DI DISPOSITIVO AZIENDALE

Con riguardo ai dispositivi di lavoro forniti dal Titolare, lo strumento è già predisposto con misure tecniche per la sicurezza delle informazioni. Il lavoratore, per parte sua deve rispettare le seguenti misure di sicurezza[1]:

- non è consentito modificare le impostazioni preconfigurate sul dispositivo dall'Ufficio IT;
- è assolutamente vietato condividere il dispositivo e/o le credenziali di accesso;
- è vietato installare *software* o applicativi non autorizzati;
- è vietato la navigazione in siti non attinenti al lavoro;
- è vietato accedere ad eventuali *webmail* personali;
- è vietata l'apertura di allegati sospetti;

ATTENZIONE A…

[1] **IN CASO DI DUBBI O NECESSITÀ DI CHIARIMENTI DI QUALSIASI TIPO E OPPORTUNO FARE RIFERIMENTO ALL'UFFICIO AMMINISTRAZIONE, NON È AUTORIZZATA L' "*AUTOGESTIONE*"**

Si ricorda che la gran parte delle minacce informatiche **ha origine dalle e-mail**, veicolo prediletto dai cybercriminali per diffondere *malware*. Fin dall'inizio della diffusione dell'epidemia, vi sono state numerose campagne **di** *phishing* **a tema Covid-19**, che nel corso di questi mesi hanno finito per mietere un quantitativo impressionante di vittime, assumendo le sembianze ad esempio di presunti bollettini sanitari, offerte di beni scarsamente reperibili, quali farmaci salvavita, dispositivi di protezione individuale, tamponi e test virologici, comunicazioni urgenti di amministrazioni fiscali, previdenziali o sanitarie, nonché comunicazione urgenti di banche.

Si invitano pertanto i lavoratori a prestare massima attenzione alla provenienza dei messaggi, verificando se l'organizzazione cui appartiene il mittente esista davvero, cercando conferme sul web o sui social media, il tenore del testo, in quanto da una semplice ma attenta lettura, è possibile cogliere incongruenze logiche, spesso dovute a traduttori automatici, nonché la presenza di link sconosciuti o di allegati sospetti. In caso di dubbio su tali situazioni, il lavoratore deve essere istruito e chiedere il da farsi ai propri referenti IT, evitando qualsiasi iniziativa personale.

È inoltre opportuno prestare attenzione a non inviare per errore informazioni aziendali o soggette al segreto professionale a terzi, non autorizzati a riceverle.

Per proteggersi è importante tenere a mente e rispettare le seguenti regole di comportamento:

- **Non utilizzare la e-mail aziendale per usi privati**: quali e-mail con gli amici, acquisti online (Amazon, eBay, shopping online in generale), partecipazione a liste informali e non istituzionali di discussione, iscrizione a siti non istituzionali, Facebook, Google, Dropbox, LinkedIn e altre piattaforme di social network. Ciò comporta la circolazione e l'esposizione pericolosa dell'indirizzo istituzionale in ambiti dove operano malintenzionati alla ricerca di potenziali vittime. Un simile comportamento può anche sollevare, in molti casi, un problema di immagine e di reputazione per l'azienda.

- **Non bisogna mai rispondere a messaggi di posta elettronica che richiedano l'autenticazione** con le credenziali aziendali o domandino esplicitamente dati, credenziali, numeri di carta di credito, informazioni correlate al dipendente o al suo account. Nessun Amministratore e nessun Ente o azienda (società informatica, banca, Agenzia delle Entrate, Poste Italiane, Equitalia o Procura) richiede oggi, tramite e-mail, tali dati. Sono tutte richieste truffaldine, che mirano ad ottenere dette informazioni.

- **Non aprire mai allegati non attesi o il cui invio non sia stato concordato con il mittente**. Spesso gli allegati servono per veicolare virus informatici o programmi che permettono a malintenzionati di entrare nel sistema. In ogni caso, prima di aprire qualsiasi allegato è sempre necessario effettuare una scansione preventiva del file allegato utilizzando l'antivirus installato sul proprio computer.

- **Verificare sempre ortografia e sintassi nel testo delle e-mail ricevute**. Spesso le e-mail ricevute contengono banali errori di ortografia, sintassi, traduzioni dall'inglese approssimative che immediatamente devono insospettire il destinatario. Si tratta infatti di e-mail standard che vengono inviate contemporaneamente a milioni di potenziali vittime.

- **Diffidare di mail che mettono urgenza, che minacciano sanzioni, che promettono premi e vincite o che contengono richieste di aiuto**. Un modo efficace che i criminali usano per convincere il soggetto a rispondere, a cliccare su un link o ad aprire l'allegato è quello di mettere urgenza, per impedirgli di pensare. Quindi, non rispondere a e-mail che minacciano sanzioni, che annunciano premi, che chiedono di fare qualcosa in fretta, che contengono richieste di aiuto umanitario, che propongono relazioni sentimentali o fugaci incontri.

- **Non cliccare su collegamenti contenuti nel testo di e-mail inattese**. Il link può condurre a siti web capaci di carpire informazioni o di infettare il computer del dipendente. Anche se il link riporta il nome di un sito noto e affidabile si può facilmente verificare qual è il sito realmente indirizzato passando il puntatore del mouse sul link (senza cliccare) e verificando in basso sul browser l'indirizzo reale: quasi sempre è diverso. Prestare particolare attenzione ai collegamenti a siti web che richiedono informazioni personali, anche se l'e-mail sembra provenire da una fonte legittima, perché i siti web di phishing sono spesso repliche esatte di siti web legittimi.

- **Non vergognarsi e segnalare subito l'incidente**. In caso di comportamento sbagliato, non vergognarsi per l'accaduto mantenendo il silenzio, ma informare subito l'Ufficio IT e il proprio responsabile della avvenuta fuoriuscita di dati all'esterno. Se si sospetta di aver comunicato le credenziali a un sito truffaldino cambiare immediatamente la password utilizzando un dispositivo diverso e scegliendone una sufficientemente robusta e avvisare tempestivamente il referente informatico e l'Ufficio IT. Usare sempre password univoche, di lunghezza adeguata, composte da caratteri minuscoli, maiuscoli, numerici e speciali; non inserire nelle password elementi banali o riferimenti personali (es. nomi, date) perché rendono la password semplice da indovinare.

- **Diffidare anche di e-mail personalizzate**. La e-mail ingannevole può essere anche personalizzata con informazioni relative al nostro ufficio o alla nostra persona: sono tutte informazioni che si possono reperire agevolmente sui social network o da elenchi pubblici (ad es. sul sito internet aziendale sono pubblicati alcuni dati relativi al luogo di lavoro, ruolo, numero di telefono e simili). Ciò significa che, anche se la e-mail dovesse sembrare realmente diretta a noi, ci si rivolga usando il nostro nome di battesimo o si riferisca a compiti, documenti, fatture, servizi o uffici di nostra competenza, occorre mantenere alta l'attenzione.

LA GESTIONE DEGLI INCIDENTI

Si definisce **DATA BREACH** un incidente di sicurezza in cui dati personali vengono consultati, copiati, trasmessi, cancellati, rubati o utilizzati da un soggetto non autorizzato.

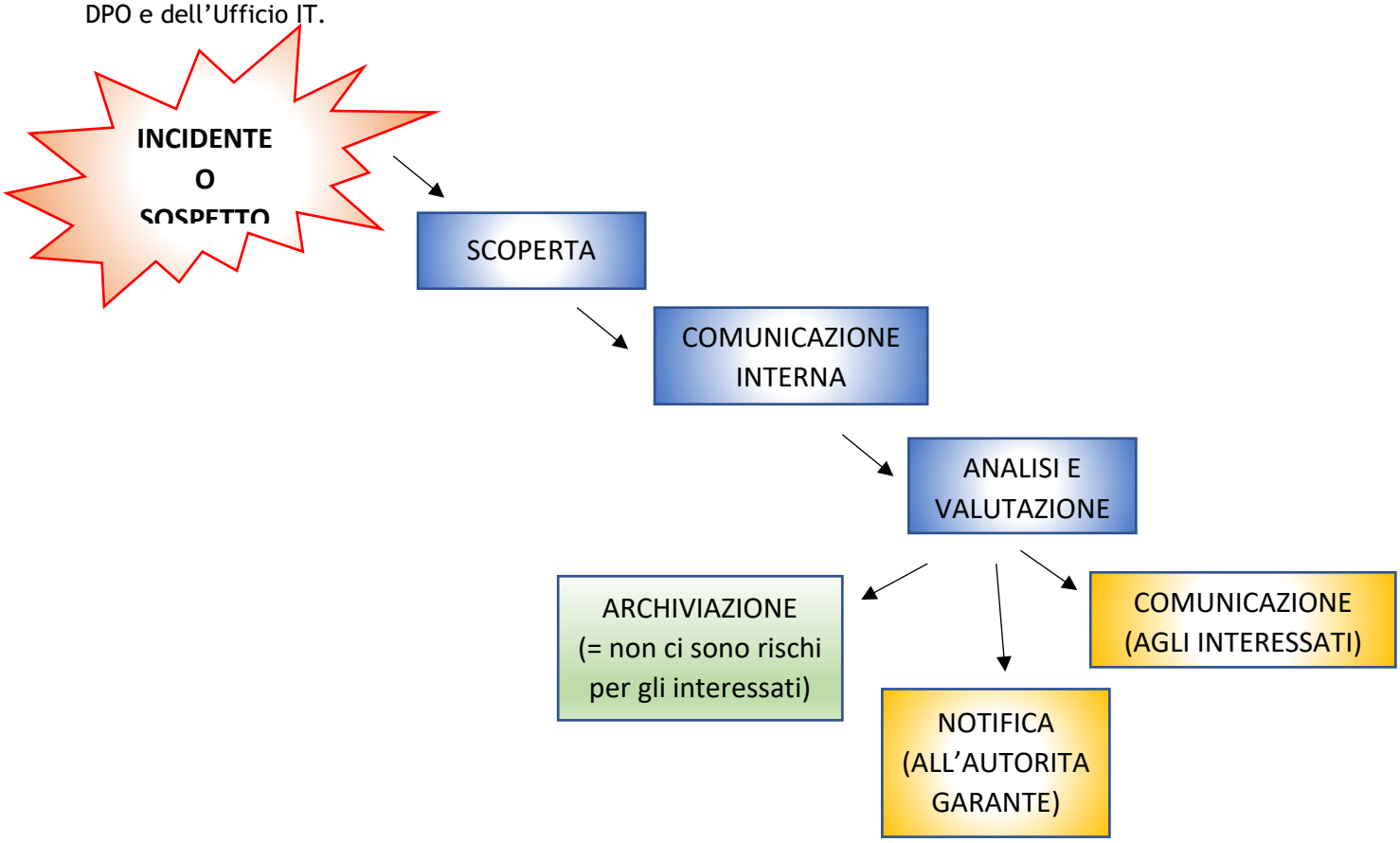
Esempi di possibili data breach:

- Smarrimento di una chiavetta USB contenente dati riservati;
- Furto di un notebook contenente dati confidenziali;
- Persona interna all'azienda che, avendo autorizzazione ad accedere ai dati, ne produce una copia distribuita in ambiente pubblico;
- Accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite.

Parliamo quindi di perdita di **riservatezza**, **integrità**, **disponibilità** di dati personali.

Nel caso in cui uno degli autorizzati al trattamento si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il proprio Responsabile e la Direzione generale.

Questi procederanno poi ad attuare la procedura per la gestione dei data breach con il coinvolgimento del DPO e dell'Ufficio IT.



Per qualsiasi domanda o necessità di approfondimento o chiarimento in relazione a quanto spiegato nel presente fascicolo informativo scrivere a: **ilaria.galante@gruppopk.com**

Allegato 2

Relazione tecnica sui sistemi informatici.

revisione 1° maggio 2023

Descrizione degli strumenti elettronici utilizzati:

L'azienda dispone di:

1 Server

26 Personal Computer / Notebook

10 tablet aziendali

I Personal computer sono identificati da delle sigle del tipo "PC-CRCXX" (dove XX è un numero progressivo assegnato alla postazione, mentre gli utenti sono identificati con la stesa sigla omettendo il prefisso PC (es: CRCXX, dove XX è sempre il numero progressivo assegnato all'operatore)

La sigla CRC si riferisce invece alla sigla aziendale (in origine Casa Riposo Castions)

Ogni PC è configurato per una sola persona e tutte le impostazioni fatte sul singolo Pc si riferiscono strettamente all'utente che ci lavora.

In linea di massima ogni PC è configurato per una sola persona e tutte le impostazioni fatte sul singolo Pc si riferiscono strettamente all'utente che ci lavora, con alcune eccezioni in cui il dispositivo viene condiviso tra più utenti. In questo caso ogni utente ha un suo profilo dedicato ed indipendente con delle proprie credenziali ignote agli operatori degli altri profili. I tablet aziendali sono vengono utilizzati esclusivamente per la gestione dei pazienti e sono integrati con il software INSOFT.

Descrizione della rete informatica aziendale

I PC sono connessi tra di loro tramite una rete di tipo Ethernet (cablata con cavi UTP RJ45) che si dirama usufruendo di uno switch centralizzato e gestibile da remoto.

Lo switch è situato in una stanza apposita dove si trova anche il server principale e si tratta di una stanza che può essere chiusa a chiave in quanto dotata di serratura; i dati sono archiviati solo sui server, sui dischi fissi dei singoli PC non è salvato alcun tipo di dato di rilevanza aziendale.

Rete Wireless

Nell'intera struttura è presente un sistema integrato Wireless servito da Access Point con tecnologia Mesh. Tale sistema è dotato di Roaming, quindi l'accesso avviene automaticamente e indipendentemente dalla posizione in cui si trova il dispositivo mobile (non è necessario cambiare manualmente il SSID). La password di accesso viene assegnata dagli incaricati solo agli utenti autorizzati. Nell'asilo e negli uffici invece vi sono delle reti Wireless separate ed inerenti alla sola attività relativa; gli access point che servono l'asilo sono 5 mentre quelli che servono gli uffici sono 2.

Internet e posta elettronica

La connessione ad Internet avviene tramite una connessione Telecom in fibra FTTC che viene utilizzata per l'attività lavorativa ordinaria. I router che gestiscono le connessioni sono collegati ad un Firewall aziendale Nethesis che applica tutte le politiche di filtraggio e protezione da accessi indesiderati; le politiche di filtraggio sono state personalizzate per il tipo di attività inerente all'azienda. Gli accessi esterni da parte degli utenti autorizzati avvengono tramite accesso VPN con certificato univoco di collegamento.

Tutti i pc della rete aziendale hanno possibilità di accesso ad internet seppur alcuni di loro ne hanno limitate le funzioni (disabilitazione cookies, controlli ActiveX ecc.).

La posta elettronica viene interamente gestita dal Mail server interno Kerio Connect il quale si occupa dello scaricamento e del reindirizzamento della posta alle corrispondenti caselle di ogni utente. Il dominio attuale di posta dell'azienda è micolitoscano.it, la posta viene scaricata dal provider di servizi tramite protocollo POP3. Il sistema di messaggistica è dotato di un ottimale filtro anti-SPAM, di un antivirus in-line (controlla i virus nei messaggi di posta prima che questi giungano a destinazione) e di parecchi filtri di controllo che vengono costantemente e automaticamente aggiornati. Le caselle di posta sono distinte per ogni utente e sono protette da password di accesso. Vi è integrato anche un sistema di messaggistica istantanea interna che permette la rapida comunicazione con gli utenti in quel momento attivi e presenti al computer.

Tutta la posta elettronica è archiviata sul server e non sui singoli pc; questo consente il salvataggio centralizzato giornaliero in modo automatico.

Funzioni e caratteristiche del server

Il server (denominato SERVENTE) ha funzioni di archiviazione dei dati dell'intera rete aziendale, sia per quanto riguarda i dati gestionali, sia per quelli di Office Automation. Dispone di due dischi SSD da 980Gb ad alta velocità che sono strutturati tra si loro per formare un sistema di "Fault Tollerance" di tipo RAID 1 (i dati vengono ripartizionati sui due dischi in tempo reale, in tal modo si salvaguardano dall'eventuale rottura fisica con possibilità di sostituzione disco mentre l'utente (nel frattempo che si provvede alla sostituzione) non viene interrotto nell'attività lavorativa in quanto il lavoro continua sul disco alternativo; il sistema prevede la sostituzione "a caldo" (senza interruzione dell'attività del server).

Principali software utilizzati a livello aziendale

- Software di Office automation (*Microsoft Office varie versioni*) su ogni postazione della rete aziendale
- Gestionale ESolver con database residente sul Server aziendale
- Software per la gestione della cartella clinica *INSOFT* con database in Cloud su archivi regionali
- Presenze Web – gestione timbrature e presenze

Criteri di protezione accessi

Ogni PC è protetto da password univoca impostata e verificata direttamente dal server principale; tale password è stata assegnata in base alla formulazione privata eseguita da ciascun utente della rete locale e segue il criterio delle password composte, è minimo di 8 caratteri.

Non segue una logica di composizione ma è frutto della fantasia di ciascuno.

Esiste una password di amministratore uguale su tutti i PC e nota soltanto agli amministratori del sistema.

In base all'utente sono assegnati i diritti di accesso alle cartelle dati presenti nel server; per quanto riguarda l'asilo invece, è stato predisposto un NAS apposito e dedicato all'interno del quale vengono gestiti gli archivi a loro dedicati.

Criteri e modalità di ripristino della disponibilità dei dati.

Gli archivi aziendali risiedono tutti nel server principale, nessun utente della rete aziendale è autorizzato al salvataggio di dati riguardanti l'attività aziendale sui pc client.

I salvataggi dei dati vengono eseguiti alternativamente su due dispositivi NAS di rete (in modo di ridurre anche il rischio dovuto a guasti di periferica) e l'operazione è eseguita ogni giorno ad orari prestabiliti nel corso della notte; non è necessario nessun intervento da parte degli utenti in quanto la procedura è completamente automatizzata. Esiste un servizio di monitoraggio in essere messo a punto dalla stessa Sistema Ufficio Srl che si occupa di verificarne la corretta esecuzione giornaliera e una console di monitoraggio centralizzata per una

visione immediata della situazione. Attualmente non è presente nessun servizio di salvataggio esterno su Cloud.

Assistenza remota

La Fondazione Micoli Toscano usufruisce di un'assistenza remota su ogni PC della rete aziendale che le consente di risolvere rapidamente qualsiasi esigenza o problematica software che si possa verificare. L'accesso del softwarista informatico incaricato avviene previo consenso dell'utente richiedente.

Protezione sistemi

Il sistema informatico è protetto dal firewall Nethesis Nethsecurity S20 con a bordo installati i servizi in abbonamento annuale per la protezione dei dati dotato di Firewall, Intrusion Detection System, VPN, Antispam, filtro siti web, gestione traffico in rete, Antivirus, interfaccia web di amministrazione, monitoraggio centralizzato, aggiornamento continuo e report accessi. I servizi vengono rinnovati con cadenza annuale ed in tale occasione viene anche effettuato l'aggiornamento dell'apparato con i "Major Upgrade" rilasciati dal produttore.

La sicurezza inoltre è implementata dall'antivirus Webroot Secure Anywhere con tecnologia Cloud based. Webroot Secure Anywhere è la soluzione antivirus che protegge in tempo reale dispositivi endpoint e mobili contro le minacce malware, garantendo la riservatezza e integrità dei dati aziendali. Lavora in tempo reale senza necessità di aggiornare le firme; è gestito direttamente nel Cloud tramite una console di amministrazione e garantisce la sicurezza completa dei dispositivi, intercettando anche virus sconosciuti.

La protezione della posta elettronica avviene tramite le caratteristiche di sicurezza integrate del mail server Kerio Connect che si riassumono nelle seguenti funzioni:

- Potente sistema di protezione via cifratura SSL e S/MIME. Sofisticato filtraggio anti-spam con blocco automatico dei server spam sconosciuti e con possibilità di classificare server conosciuti in whitelist

- Protegge la rete, intercettando virus, Trojan e spyware presenti nelle mail in entrata, in uscita e scambiate internamente mediante il Sophos anti-virus integrato.

- Blocca gli IP sospettati di provare ad indovinare le password; blocca gli account attaccati ma non considera attacchi i tentativi provenienti dalla rete locale.

- Sfrutta il protocollo Kerberos per autenticare i tentativi di log-in tra più server o tra client e server.

- Respinge gli attacchi di Hacker e attività sospette filtrando e vietando la consegna di allegati in maniera automatica. Blocca i tentativi di abuso delle mail utilizzando tecnologie integrate.

Sistema di archiviazione della posta elettronica

Vi è residente inoltre un sistema di archiviazione della posta elettronica che si occupa di archiviare automaticamente la posta più datata in un apposito datastore situato sempre sul server. Tale datastore è protetto e non accessibile da parte degli utenti ma solo direttamente dal software Mailstore che si occupa dell'archiviazione. I messaggi vecchi possono pertanto essere consultati dagli utenti senza dover impegnare necessariamente il client di posta elettronica, che mantiene così le sue prestazioni ottimali. Tale sistema di archiviazione è conforme alle normative GDPR (conservazione, protezione e cancellazione sicura dei dati)

Suggerimenti per l'implementazione e miglioramento delle sicurezze internet

In tempi in cui gli attacchi informatici sono sempre più frequenti e i dati aziendali sono messi continuamente a rischio di criptazione, furto e manomissione; la Sistema Ufficio Srl è in grado di fornire strumenti avanzati per il miglioramento della sicurezza aziendale. E' quello che fa il nostro "Filtro Contenuti e Malware", il filtro internet nella nuvola, semplice, e completamente in Italiano, che funziona totalmente in rete. È configurabile ed integrabile su ogni tipologia di rete e compatibile con qualunque Router, HotSpot Wi e Firewall.

· Filtra i siti non idonei all'attività lavorativa

· Blocca i siti infetti che causano problemi ai pc

· Elimina le perdite di tempo durante l'orario di lavoro

· Aiuta le imprese a rispettare il GDPR (Regolamento privacy europeo)

Allegati riguardanti la rete informatica

Si fornisce in allegato un plico di prospetti dettagliati riguardanti le apparecchiature informatiche e i software di protezione impiegati nella struttura

Tali prospetti si riassumono in:

- Elenco degli elaboratori e descrizione degli stessi

- Prospetto riepilogativo antivirus e ultime minacce rilevate